CENTRAL EUROPEAN UNIVERSITY

THE PROTECTION OF FUNDAMENTAL RIGHTS ONLINE: FREEDOM OF EXPRESSION AND INTERMEDIARY SERVICES PROVIDERS SECONDARY LIABILITY IN THE EUROPEAN UNION

by Natalia Mileszyk

LL.M. THESIS
PROFESSOR: Dr. Kristina Irion
Central European University
1051 Budapest, Nador utca 9.
Hungary

I would like to express my gratitude to Dr. Kristina Irion
for being a very encouraging and inspiring advisor.

A very special thanks goes to Robin Bellers for his patience
and support.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The blocking of twitter users, unwanted content on webpages or controversial comments on blogs – these are only a few examples how private actors censor content online. In the European Union the issue becomes more burning and widespread, since the E-Commerce directive makes the implementation of notice and take down procedure a defence against secondary liability of Intermediary Service Providers (ISPs).The impact of this procedure on limitation of freedom of expression is significant - the authors of publications are deprived of the right to prove if the content should never be blocked.

Due to the fact that human rights do not bind private entities (ISPs are not responsible for human rights protection) the state should regulate possible interference of ISPs in such a way that their discretion is minimal. The paper analyses the legal framework of ISP liability in the European Union, the Council of Europe and Poland. It finds that EU member states within the process of regulating ISP liability did not fully take into consideration their human rights obligations. The thesis concludes that the state has positive obligation to legislate ISP secondary liability in order to protect freedom of speech against arbitrary decisions by ISPs and EU member states failed in this respect. The thesis supports this contention with an examination of both legislative measures and judicial decisions.

So far the question of legal liability for Internet Service Providers for unlawful user generated content was mostly discussed from an economic or technical perspective – human rights aspects were neglected. The thesis, by closely examining the legal framework and practice in the European Union, the Council of Europe and Poland sheds new light on the rarely acknowledged issue of the interrelation of ISP liability and freedom of expression.

INTRODUCTION

The Internet influences various aspects of our everyday life, ranging from the work environment, through access to services, to the way we spend our leisure time. Professor Staples noticed that "netizens"[1] start to perceive online activity as crucial as real one.[2] Unsurprisingly, such progress also influences the environment of human rights. Through access to information people become more aware of their rights, global actions[3] and protest are easier to organize, and monitoring of governments' actions is less challenging. Therefore, human rights activists benefit from networking.

Notwithstanding a "tool related" approach to the relation between human rights and the Internet, the other dimension must be also borne in mind: the exercising of freedoms online. Primarily it was believed that the Internet is a final solution for various limitations and restrictions imposed by states on human rights – it was perceived as a chance to create a zone for exercising various rights without any interference.[4] The reality and practice in the 21st century has shown something totally different. Abuses of digital rights are more common and widespread than ever, data retention, internet access blocking and criminal prosecution to name only

[1] A term coined on the Internet to describe users "*who utilize the networks from their home, workplace, or school (among other places)*", Wikipedia, the Free Encyclopedia, Netizen, http:// en.wikipedia.org/wiki/Netizen, last accessed on 25 September 2013.
[2] Staples, William G., "Everyday Surveillance: Vigilance and Visibility in Postmodern Life", Rowman& Littlefield Publishers, 2000, p.130.
[3] With the best example of Amnesty International and its Urgent Actions.
[4] Norris, Pippa, "Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide", Cambridge: Cambridge University Press, 2001, pp. 232-33.

a few examples.[5] It seems that the more aware of the Internet's power and possibilities states are, the more authorities try to take control over it.

The thesis deals with the very specific issue of the Intermediary Service Provider secondary liability (hereinafter ISP liability). Seemingly, it is a only technical regulation related to e-commerce. I argue that in EU member states a positive obligation of the state concerning the legislation process of ISP liability in the area of fundamental rights exists (especially when freedom of expression is at stake). The scope of the obligation is to enact laws that will minimize ISPs' discretion impacting freedom of expression of online users. The problem is not so abstract as it might seem – on 14 February 2013, the Court of Appeal of England and Wales[6] stated that Google can be liable for comments posted on its Blogger platform if it does not imply the notice and take down procedure.

The characteristic feature of the Internet is the fact that information and content are transmitted via channels provided by third parties.[7] As intermediary service providers we understand the entities (usually commercial, but sometimes also individuals or NGOs) providing access to the Internet. Three basic types of ISPs recognized in the literature are: access, hosting and transit.[8] In the thesis, using the expression "ISP" I usually refer to hosting ISP – the one able to store content, especially via web-hosting services. From a technical point of view ISPs play

[5] Deibert, Roland and NartVilleneuve, "Firewalls and Power: An Overview of Global State Censorship of the Internet" in: Matthias Klang and Andrew Murray, "Human Rights in the Digital Age", London: GlassHouse, 2005, pp.111-115.
[6] The Court of Appeal of England and Wales, *Tamiz v Google Inc*, [2013] EWCA Civ 68, available at: http://www.bailii.org/ew/cases/EWCA/Civ/2013/68.html, last accessed on 25 September 2013.
[7] Perset, Karine (Organization for Economic Cooperation and Development), "The Economic and Social Role of Internet Intermediaries", April 2010, e DSTI/ICCP(2009)9/FINAL, available at: http://www.oecd.org/internet/ieconomy/44949023.pdf, last accessed on 25 September 2013.
[8] Cohen-Almagor, Raphael, "Freedom of Expression, Internet Responsibility and Business Ethics: The Yahoo! Saga and Its Aftermath", *Journal of Business Ethics*, 21 July 2011, pp. 353-365.

the role of online "gatekeepers".[9] The access to a network without their commercial services is impossible, but on the other hand their role is usually purely automatic. This also emphasizes why the topic of the thesis is so crucial.[10]

Secondary liability is a legal construction when somebody is held liable for the action of other persons due to some structural or functional connection. In the case of the Internet we use this term when somebody providing services is liable for the actions of the users.[11]

The notice and take down procedure (being an example of notice and action procedure) derives originally from the copyright infringement regulation in the US, but nowadays is applied in various types of situations.[12] This is a procedure when the host of the content takes action (removes it or blocks) after receiving a notification (or court order) about the allegedly illegal content.

The impact of this procedure on limitation of freedom of expression is significant. First of all, the authors of publications are deprived of the right to prove that the publication should not be the subject to the notice and take down procedure. Furthermore, there is a threat that ISPs will be discriminative in their activity and create additional requirements for persons willing to use their hosting services.[13] Due to the fact that human rights do not bind private entities (ISPs

[9] Demont-Heinrich, Christof, "Central points of control and surveillance on a "decentralized" Net: Internet service providers, and privacy and freedom of speech online", *Info*, Vol. 4 Iss: 4, pp. 32 -34.
[10] As mentioned: "ISP's power and status call for careful consideration and clarification" – Cheung, Anne and Rolf Weber, " Internet governance and the responsibility of Internet Service Providers", Summer 2008, 26 *Wisconsin International Law Journal* 403, p. 405.
[11] Smith, Emerald, "Lord of the Files: International Secondary Liability for Internet Service Providers", *Washington & Lee Law Review* 68(3), pp.1555-1588.
[12] The procedure was firstly introduced in Millennium Digital Copyrights Act, US legislation on IP protection, Pub. L. 105-304, 112 Stat. 2860; more on the issue in the context of the thesis: Medenica, Olivera and Kaiser Wahab "Does liability enhance credibility? Lessons from the DMXA applied to online defamation", 25 *Cardozo Arts & Entertainment Law Journal*, pp. 237-270.
[13] Iulia-Barcelo, Rosa and Kamiel Koelman, "Intermediary Liability in the E-commerce directive: So Far so good, but not enough", *Computer Law and Security Report* 2000-4, pp. 231-239.

are nor responsible for human rights protection) the state should regulate possible interference in such a way that discretion is minimal.

There are many legal aspects related to ISP liability which I do not address in the thesis due to the breadth of the topic. To tackle ISP liability concerns holistically, it is necessary to elaborate also on the issue of direct liability online, the borderless nature of the Internet[14] and the jurisdiction in the Internet[15]to name just a few problems.

I will focus on the situation of defamation online, so the situation where human rights clash on the internet and what actions of ISPs are legal in such situations (and if all of them are legal also from a human rights perspective). It is worth emphasizing that legal actions aimed at deciding which right should prevail in a certain clash situation (for example against the author of publications that contain slander, defamation, etc.) might be challenging, or sometimes even impossible. Therefore the third part – ISPs –also become involved by notice and take down procedure. The crucial question is how to balance this mechanism with freedom of expression and what the role of the state and private entities is in this aspect.

The first chapter is devoted to ISP liability in the EU. I argue that the E-Commerce directive and the way it was implemented in national legal systems creates the situation of legal uncertainty which threatens freedom of expression of the users. Afterwards I address the issue of the Internet as an environment for exercising and abusing human rights. I argue that the significance of the Internet in this area increases and analyse Internet impact on the human rights framework, especially freedom of expression and right to privacy protection in the Council

[14] Akdeniz, Yaman, "To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression", (2010) *Computer Law andSecurity Review*, Vol. 26(3), May, pp. 260-273.
[15] Uerpmann-Wittzack, Robert, "Principles of International Internet Law," 11 *German Law Journal*, (2010), p.1253; Reed, Alan "Jurisdiction and choice of law in a borderless electronic environment" in YamanAkdeniz, Clive Walker and David Wall (eds.) "The Internet, Law and Society", Longman, 2000; Reidenberg, Joel "Technology and internet jurisdiction", *University of Pennsylvania Law Review*, 2005 Vol. 153, p. 1951.

of Europe (CoE). I tackle also the issue of self-censorship online and permissible limitation of human rights. Chapter three is a case study of the chosen member state: Poland, its legislation and judicial decisions on ISP liability. I conclude that the way the directive is implemented does not secure freedom of expression sufficiently. The last chapter, concluding observations and comments from previous parts, deals with the issue of human rights aspects of ISP liability framework and practice in the CoE, the EU and Poland. The one difference between the EU and CoE needs to be understood – the aim of provisions covering the same situation – the EU's main objective is to establish a free market and reinforce interstate cooperation mostly on the economic level. The aim of the CoE is to protect human rights. Therefore Polish authorities by being obliged to implement both law systems' provisions have to try to strike a balance when achieving these two, usually competing rights. I conclude that there is a positive obligation of EU member states to protect freedom of expression online via proper ISP liability framework and generally countries have failed to comply with this.

The thesis is an answer for the social and political problem that is currently very visible – the ISPs, private entities, can easily interfere in exercising freedom of expression online. Therefore the understanding of the problem is necessary before the legal comparison. It is also the reason why I finish my thesis with certain and specific propositions about legal solutions which should be taken by member states and most preferably also at EU level.

The matter of human rights dimension of ISP secondary liability is well-established among American scholars.[16] It might be explained by the developed, compared to the EU, regulation of secondary liability in the Digital Millennium Copyright Act and very extended

[16] E.g. Balkin, Jack M."Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society", *New York University Law Review,* Vol. 79, No. 1, 2004; Mann, Ronald J. and Seth Belzley, "The Promise of Internet Intermediary Liability", *William and Mary Law Review*, Vol. 47, October 2005.

protection of ISPs – they might be held liable only in very restricted cases of copyright infringement. Unfortunately, so far only a few European authors emphasized the importance of evaluation of the E-Commerce directive from a human rights perspective,[17] which seems surprising especially taking into account that in the EU ISPs might be responsible in case of any violations.[18] The thesis therefore addresses the issue of ISP liability in the EU with special attention to defamation cases, contributing to the discussion on human rights aspects of ISP liability.

[17] E.g. Cheung, Anne and Rolf Weber, "Internet governance and the responsibility of Internet Service Providers", Summer 2008, 26 *Wisconsin International Law Journal* 403; Tambini, Damian, Danilo Leonardi and Christopher Marsden, "Codifying Cyberspace : Communications Self-Regulation in the Age of Internet Convergence, New York: Routledge, 2008, p. 281.

[18] The general conclusion from Splinder, Gerard (ed.) "Study on liability of Internet Intermediaries", 12 November 2007, Markt 2006/09/E, Service Contract ETD/2006/IM/E2/69, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf, last accessed on 15 November 2013.

CHAPTER 1 - INTERMEDIARY SERVICE PROVIDERS SECONDARY LIABILITY IN THE EUROPEAN UNION

Intermediary Service Providers secondary liability is definitely not an issue associated by the majority with human rights. But one of the aims of the thesis is to evaluate this legal, seemingly business construction, from a human rights angle. Therefore the chapter is dedicated to building the understanding of ISP secondary liability, not only as a human rights phenomena, but more importantly as a regulation playing the fundamental principal role in the way business nowadays works. Without answering the preliminary question: "how responsible are those who provide Internet Service for the actions of those who use those services?"[19]it is impossible to elaborate on the impact of the whole ISP secondary liability regime for freedom of expression online.

Secondary liability online rose to a high position on the agenda of the EU due to very prosaic reason – in the Internet, which mostly facilitates anonymous activities, it is always much easier to sue an ISP than any user.[20]Moreover, due to the well-developed data protection regime in EU, sometimes this is even the only possible solution for somebody whose right was infringed.[21]

[19] Smith, Emerald; "Lord of the Files: International Secondary Liability for Internet Service Providers"; *Washington & Lee Law Review* 68(3), 2011; p.1555.
[20] Okoń, Zbigniew, „Oskarżony: ISP odpowiedzialność dostawcy usług internetowych" [Accused: ISP. Liability of service providers]; 1 December 2000; available at: http://www.internetstandard.pl/artykuly/277675/Oskarzony.ISP.odpowiedzialnosc.dostawcy.uslug.internetowych.html; last accessed on 2 November 2013.
[21] Pacek, Grzegorz Jarosław; „Wybrane zagadnienia związane z odpowiedzialnością dostawców usług hostingowych" [Chosen aspects of ISP secondary liability]; *Monitor Prawniczy* 4/2007; p.2.

The chapter builds understanding of ISP secondary liability by explaining the regulation in the EU – both on community and national levels. The chapter focuses mostly on EU legislation, jurisprudence and the question of implementation of the directive in member states legal frameworks. The issue of litigation in national courts (on Polish example) is addressed in Chapter 3 (with only a few decisions mentioned in this chapter where this is inevitable).

The chapter begins with a brief summary of the E-Commerce directive and reasons behind its enactment. Afterwards, the specifics and scope of ISP legislative safe harbour is presented. After depicting the legal situation on EU level, it is possible in part three to elaborate on the way the directive was implemented in Poland. The chapter provides also an overview of selected jurisprudence of the Court of Justice of the European Union (CJEU). Such a broad perspective on the topic lays the ground for the conclusions that ISP liability regulation in the EU, its legal gaps and question marks that interpretation can result in a situation of insufficient human rights protection, which is the subject of the following chapters.

1.1. The E-Commerce directive[22] as a legal measure taken at EU level

The E-Commerce directive, adopted in 2000, is the first legal community measure to establish a common framework for rapidly developing electronic commerce. The section elaborates on legal discrepancies before adopting the measure and reasons behind creating the directive and choosing an issue of ISP secondary liability to be regulated in the directive.

[22] 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, 17.7.2000, pp. 1–16.

1.1.1. ISP secondary liability in member states before the E-Commerce directive

The rising popularity of the Internet forced states to face various legal challenges. The question how to treat ISPs was one of them. Many countries relied on publishers' liability rules.[23] Such an approach was vividly criticized taking into consideration a lack of publisher (ISP) scrutiny.[24] Some other countries adopted specific liability legislations.

The United Kingdom as early as 1996 adopted the Defamation Act[25] which contained "innocent dissemination" – the defence which could be used by an ISP in the case a provider could prove "reasonable care" while conducting its activity. The scope of the provision was later narrowed by courts, deciding that lack of action after being informed about a defamatory statement makes it impossible for ISPs to raise a defence.[26] The British approach to the issue was an inspiration for EU legislation.

The Netherlands is an example of a country that regulated ISP liability through courts' rulings, not specific legislation. In the Scientology case,[27] the Court found several ISPs not liable for enabling the posting of copyrighted works on their webpages. The court stated that ISPs lack

[23] High Court, Queen's Bench Division (UK), *Godfrey v Demon Internet Service* [2001] QB 201; the case is related to defamatory content posted on a newsgroup, the Court found that ISP can be liable as publisher for libel since "posting" equals "publicizing".
[24]Splinder, Gerard (ed.) "Study on liability of Internet Intermediaries", 12 November 2007, Markt 2006/09/E, Service Contract ETD/2006/IM/E2/69, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf, accessed on 15 November 2013, p. 47.
[25] It was the first European legislation addressing directly the issue of ISPs secondary liability – An Act to amend the law of defamation and to amend the law of limitation with respect to actions for defamation or malicious falsehood, 1996 c 31, available at: http://www.legislation.gov.uk/ukpga/1996/31/contents/enacted.
[26] Splinder, Gerard (ed.) "Study on liability of Internet Intermediaries", 12 November 2007, Markt 2006/09/E, Service Contract ETD/2006/IM/E2/69, http://ec.europa.eu/internal_market/e commerce/docs/study/liability/final_report_en.pdf, accessed on 15 November 2013, p. 47.
[27] The District Court of Hague (The Netherlands - Rechtbank Den Haag), *Scientology vs. providers and others* 96/1048, 9 June 1999.

the ability to influence the content and their main activity is to provide a platform for public disclosure, not to monitor or censor.

In Germany the Tele-service Act and Multimedia Law[28] was adopted in 1997. In the regulation the distinction between transmission providers and long-term storage providers was made, and therefore the catalogue of entities was very broad. Sweden decided to adopt a narrower approach by introducing in 1998 the Act on Responsibilities of Electronic Bulletin Boards.[29]The act puts on providers an obligation to monitor boards and block any illegal content.

Paralleling the borderless nature of the Internet and legislatives on ISP liability in EU member states before adopting the directive indicates with how insufficient and unrealistic legal framework ISPs (that usually conduct their business on international scale) had to deal. Such situation became unacceptable for the Community that honours and prioritizes the principle of free movement of services. Different legal approaches to the e-commerce in various member states hindered the growth in e-services sector, therefore common legal framework became inevitable and desired. As shown above, member states have already been dealing with the ISP secondary liability, but broad divergence existed not only in national legislation, but also in case law.[30] Leaving the question without harmonization on EU level could have created the dangerous situation of legal uncertainty, especially alarming in the Internet environment, where the web is "borderless" and anyone can generate content in any part of the World.

[28]Das Gesetzüber die Nutzung von Telediensten – Teledienstgesetz (Germany), 9020-6 aF, 22 July 1997.
[29] Act on Responsibility for Electronic Bulletin Boards (Sweden), SFS 1998:112, 12 March 1998, English version available at: http://www.government.se/content/1/c6/02/61/42/43e3b9eb.pdf
[30] Van Eecke, Patrick and Maarten Truyens "Liability of online intermediaries" in: "Legal analysis of a Single Market for the Information Society" (SMART 2007/0037), study of European Commission, available at:http://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037; p.6.

1.1.2. Reasons behind creating the E-Commerce directive

The EU is built on the core freedom of movement of people, goods, services and capital.[31] Starting from the 1990s, the EU had to face challenges (and also benefit from opportunities) related to the short-lived dot-com-boom.[32]The development of e-commerce is one of the results of the growing popularity of the Internet – not surprisingly people started to move services online wherever it is possible (due to it being cheaper, and the borderless nature of the Internet)[33]. In the EU the process of e-commerce becoming a more relevant policy issue can be observed.[34]

The mile-stone of e-commerce legal framework in EU development was adaptation of "A European Initiative on Electronic Commerce"[35] by the European Commission on 16 April 1997.[36] The strategy pointed 4 main areas which have to addressed on Community level. Firstly, the issue of reliable telecommunications network is named to be an issue of particular relevance. Then, bearing in mind Single Market principle, EU legislation has to be adopted to enhance e-commerce progress. The Commission stressed also the significance of providing businessmen

[31] Article 26(2) of Treaty on the Functioning of the European Union, consolidated version: OJ C 326, 26 October 2012.
[32] Christou, George; "The new electronic marketplace: European governance strategies in a globalising economy"; Edward Elgar Pub, 2007; p. 93.
[33] The e-commerce value in EU in 2012 was 312 milliard euro, according to data from the report "*European B2C Ecommerce Report 2013"* prepared by Ecommerce Europe, available at: https://www.ecommerce-europe.eu/website/facts-figures/light-version/download%20, last accessed on 20 November 2013.
[34] More on this issue: Christou, George "The EU and Internet Commerce Regulation" in: George Christou and Seamus Simpson "The new electronic marketplace : European governance strategies in a globalising economy"; Edward Elgar Publishing Limited, 2007.
[35] "A European Initiative on Electronic Commerce", Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(97)157 of 16 April 1997.
[36] Other initiatives worth noticing and relevant for information society are: the Communications Standardization and the Global Information Society, COM (96) 359 final of 24 July 96; Learning in the Information Society - Action Plan for a European Education Initiative, COM (96) 471 of 2 October 1996; Illegal and Harmful Content on the Internet, COM (96) 487 of 16 October 1996; Cohesion and the Information Society, COM (97) 7 of 22 January 1997; and the Green Papers Living and Working in the Information Society: People First, COM (96) 389 of 24 July 1996; and The Protection of Minors and Human Dignity in Audiovisual and Information Services, COM (96) 483 of 16 October 1996.

with tools and know-how about the e-commerce and the role of global regulation in securing goals set up in the strategy.

The proposal of the directive was drafted by the EU Commission's Internal Market Directorate General and the main aim of the regulation was to create a legal framework to allow e-commerce to operate on the same conditions in the whole single EU market. One of the sub-aims of a great relevance was to find fair balance how to approach the issue of ISP liability. There are also other areas addressed, such as: information requirements for ISPs, commercial communication and electronic contracts. The directive takes into account both business and consumers demands.

Currently the issue of the e-commerce and information society is of even greater weight than before. EU policy is structured around "Europe 2020 Strategy"[37] – the growth strategy for ongoing decade that introduced seven "flagship initiative". One of such initiatives is the development of digital economy, being specified by the "Digital Agenda for Europe"[38]: "the overall aim of the Digital Agenda is to deliver sustainable economic and social benefits from a digital single market based on fast and ultra fast internet and interoperable applications". On 11 January 2012, the European Commission announced "A coherent framework to build trust in the Digital single market for e-commerce and online services"[39] that sets certain, measurable goals to be achieved - one of them is doubling the volume of e-commerce in the EU by 2015.

[37] "EUROPE 2020. A strategy for smart, sustainable and inclusive growth" , Communication from the Commission of 3 March 2010, COM(2010) 2020 final.
[38] "Digital Agenda for Europe", Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of 26 August 2010, COM(2010) 245 final/2.
[39] "A coherent framework to build trust in the Digital single market for e-commerce and online services" Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of 11 January 2012, COM(2011) 942.

1.1.3. Reasons to address the issue of ISP secondary liability in the E-Commerce Directive

Negotiating article 14 of the E-Commerce directive, commissioners were aware that secondary liability is a problematic mechanism which raises questions about liability allocation.[40] On the one hand, ISPs lack technical tools to monitor every single piece of content published by their users. On the other, taking into account online anonymity, it is sometimes impossible to hold authors of the content accountable. The same dilemma was faced during negotiating press regulation – how to create liability framework and to protect anonymity of some journalists in the same time. Many legislator bodies decided to establish a registration obligation for press publishers, so even if it is not possible to sue a journalist, the civil claim can be always brought against publisher.[41]The issue of ISP liability in the EU was approached differently – the compromise was achieved that there are situations where it is not possible to held an ISP liable for user generated content.

The reasons to introduce ISP liability on EU level was summed up as follows:

"There is considerable legal uncertainty within Member States regarding the application of their existing liability regimes to providers of information Society Services when they act as "intermediaries", i.e. when they transmit or host third· party· information (information provided by the users of the service).These activities have been the subject of the different Member States' initiatives adopted or currently being examined on the issue of liability."[42]

As showed above, great discrepancy existed in legislations covering ISP liability before introducing the E-Commerce directive. Such a situation undermined principles of single market,

[40] Proposal for a European Parliament and Council directive on certain legal aspects of electronic commerce in the internal market; 98/0325 (COD); available at: http://aei.pitt.edu/13258/1/13258.pdf; p. 12.
[41] E.g. such a regulation is provided in Polish Press Law of 26 January 1984, official journal no.5 item 24, as amended.
[42] Van Eecke, Patrick and Maarten Truyens "Liability of online intermediaries " in: "Legal analysis of a Single Market for the Information Society" (SMART 2007/0037), study of European Commission, available at:http://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037; p. 12.

free movement of services and human rights protection – therefore it was decided to introduce ISP liability legal framework on EU level.

1.2. A legislative safe harbour provision in the E-Commerce directive

This section elaborates on the features and scope of ISP legislative safe harbour provisions provided in the E-Commerce directive, with special focus on article 14 which is the most relevant for this thesis.

1.2.1. The E-Commerce Directive – general remarks

The E-Commerce Directive, introduced in 2000, is the main legislative measure adopted to create common internal e-market. It "seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States".[43] The definition of information society services is derived from the directive laying down a procedure for the provision of information in the field of technical standards and regulations.[44] The notion means "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". Therefore the scope of the Directive covers only services provided without simultaneous presence of the parties involved, by means of electronic

[43] Article 1 of the E-Commerce Directive.

[44] Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Official Journal 217/18, art. 1(2).

processing and data storage such as wire, radio or optical means and such services can be provided only after individual request of the recipient.

The Directive contains Internal Market Clause which says that information society services are regulated by the legislation of the state they were established in (so called originating country rule).[45] The place of establishment is understood as the country where service "effectively pursues an economic activity using a fixed establishment for an indefinite period".[46]

The Directive aims in boosting e-commerce in the EU by legislating obligations and rights of consumers and businesses alike. It deals with the issues of transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of ISP liability. The scope of the directive covers wide range of e-services: professional services (e.g. medical consultations, selling of products and goods, information services, entertainment services, direct marketing, online advertisement, intermediary services (such as access to network) to name few examples. The directive covers services between enterprises (B2B), services between enterprises and consumers (B2C) and services of online electronic transactions. In the next part of the thesis focus will be put on articles 12-15 (section 4 of chapter II) creating rules of ISP liability.

[45] Article 3 of the E-Commerce Directive.
[46] Article 2(c) of the E-Commerce Directive.

1.2.2. A legislative safe harbour – explanatory note

A legislative safe harbour provision is one which creates exceptions from to liability. The general rule is that ISPs can be held secondary liable[47], with three exceptions provided by the E-Commerce directive. Each exception names the entities which might be excluded from liability and enumerate conditions which must be fulfilled to benefit from each safe harbour provision. Such regulations are comprised in section 4(article 12 to 15) of the E-Commerce Directive.

It is worth emphasizing that the E-Commerce directive does not create common liability regime for all Member States.[48] It only constitutes additional liability exceptions – therefore ISPs can still face different liability regimes in various parts of the EU. Moreover, it covers only "service providers", not "content providers",[49] therefore safe harbour provisions can be applied only in the case of user generated content.

The directive provides liability exceptions to three types of intermediaries, namely "mere conduit ISP" (article 12), "catching providers" (article 13) and "hosting providers" (article 14). The scope of legislative safe harbour for each type depends on the level of involvement in the content online. "Mere conduit" providers deliver services related to data transmission by network access or transmission service. Due to their purely technical role they cannot be held liable as

[47] Secondary liability is „liability that does not arise unless the primarily liable party fails to honor its obligation", the definition from Black's Law Dictionary, Thomson/West, 2005.
[48] Van Eecke, Patrick and Maarten Truyens "Liability of online intermediaries" in: "Legal analysis of a Single Market for the Information Society" (SMART 2007/0037), study of European Commission, available at:http://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037; p. 27.
[49]Rennie, Michèle, "Electronic Commerce: A Review of The European Commission's Proposed Directive", *Computer and Telecommunication Law Review*, 4/1999, p. 96.

long as their conduct is passive (there is no interference in transmission of data by ISPs by selection or modification). "Catching providers" store data only for a short time and in an automatic way. An example of such a type of ISPs is a proxy server, which stores copies of webpages accessed by a user. As long as its role remains purely passive and in accordance with conditions of access to information, an ISP is exempted from liability. "Hosting providers" store and provide access to data and are not liable under the condition that:

> "(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
> (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."

It is also significant that article 15, applicable for all types of providers, forbids countries to impose general obligation to monitor and to actively track illegal content, leaving ISPs in a simply passive role. The rule was explicitly introduced in almost all EU member states[50] and confirmed by many courts, such as the German Federal Court[51] or the Austrian Supreme Court.[52] A different approach will definitely jeopardize the role of the internet as a communication tool by hindering the work of ISPs.[53]

The question of general monitoring obligation was also addressed by the CJEU in *Sabam v. Scarlett*.[54] Sabam, the IP owners –Belgian association, wanted one of the national-wide ISP

[50] With exception of Sweden, where in Act on Responsibilities of Electronic Bulletin Boards there is an obligation placed on ISPs to monitor bulletin boards – an exception based on recital 48 of the Directive.
[51] Bundesgerichtshof (Germany), Internet-Versteigerung I, Urt. v. 11 March 2004, Az.: I ZR 304/01 – MMR 2004, 668; the court decided that the owner of auction platform is not obliged to monitor items for sale.
[52] Supreme Court of Austria, *Online Gästebuch case*, 6 Ob 178/04a; not only the court confirmed that the general obligation to monitor is against the E-Commerce directive, but also pointed at the clash of such a concept with freedom of expression.
[53] Iulia-Barceló, Rosa; "Online Intermediary Liability Issues: Comparing E.U. and U.S. Legal Frameworks"; *European Intellectual Property Review*, issue 3/2000; p. 105.
Court of Justice of European Union of 16 February 2012; *BelgischeVereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog* NV; case C-360/10.

Scarlett to install a general and unlimited in time filtering mechanism to prevent posting any content infringing intellectual property rights.

The Court confirmed that article 15 (prohibition of general monitoring obligation) also prevents installing filters *a priori* in order to avoid intellectual property infringements. No matter what kind of ISP is concerned, such a mechanism cannot be legitimate. The decision is the first in CJEU jurisprudence on ISP secondary liability that refers also to fundamental rights, such as freedom to receive and impair information and privacy, not only economic concerns.

1.2.3. A legislative safe harbour for hosting providers – Article 14 of the E-Commerce Directive

There are some features common for all schemes of legislative safe harbour provided in the E-Commerce Directive.[55] Firstly, the intermediary role is understood as passive. The level of engagement into stored data varies depending on the type of provider and in the case of hosting providers the threshold is quite low – providers can decide on what to post or to whom content should be available. Additionally, safe harbour provisions create very broad horizontal liability exceptions.[56] Therefore ISPs are not only protected from contractual liability, but also from penal, civil, administrative or extra-contractual liability.

[55] Van Eecke, Patrick and Maarten Truyens "Liability of online intermediaries" in: "Legal analysis of a Single Market for the Information Society" (SMART 2007/0037), study of European Commission, available at:http://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037, p. 8.

[56] Contrasting with US approach that has different regimes for copyright infringements (Millennium Digital Copyrights Act, 28 October 1998, Pub. L. 105-304) and defamation online (Communications Decency Act, 8 February 1996).

Article 14 solves the issue of hosting providers' liability, so services related to data storing and accessing, such as in the form of webpages. Some authors distinguish two types of hosting providers – storing materials provided by the user, such as complex webpages of the company and storing materials provided by users as a part of multi-user platform, such as discussion groups.[57] Both types of providers are covered by the directive, but the directive creates different thresholds for civil and criminal liability. Criminal liability is exempted when "the provider does not have actual knowledge of illegal activity or information" and civil when it "is not aware of facts or circumstances from which the illegal activity or information is apparent". Both kinds of liability are exempted when the ISP "upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information". Therefore, it is not enough to prove that ISP could have known about illegal activity – the threshold of knowledge is higher.

The directive does not address the issue of breaching the contract between ISPs and the user for taking down/blocking the content.[58]Except for creating a general framework of ISP legislative safe harbour, any procedural guarantees or schemes of notice and take down procedure are not provided in the directive.

[57] Kot, Dawid; „Dyrektywa Unii Europejskiej o handlu elektronicznym i jej implikacje dla prawa cywilnego" [The E-Commerce Directive and itsimplications for civil law], *Kwartalnik Prawa Prywatnego,* 1/2001; p. 93.
[58]Chissick, Michael; "Electronic Commerce: Law and Practice"; Sweet & Maxwell, 2002; p. 322.

1.2.4. Interpretation question marks related to the E-Commerce directive

Many scholars and experts raise the question of ambiguity and uncertainty of language used in the E-Commerce directive.[59] The problem creates interpretation question marks not only while discussion liability regime,[60] but also while assessing the scope of the whole directive.

1.2.4.1. Remuneration

As described above, safe harbour provisions are created for information society services, which are, according to the definition in the directive "normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

So far "remuneration" was interpreted as a wide range of economic activates in accordance with article 50 CE Treaty.[61] Nevertheless, some activities were excluded from the scope of the provision, such as public education and governmental services.[62] The question which will probably arise one day is what about services, webpages and portals (or even access to external networks) provided by public universities or governmental institutions – are they covered by liability exceptions or not? Taking into account the developing popularity

[59] Van Eecke, Patrick and Maarten Truyens "Liability of online intermediaries " in: "Legal analysis of a Single Market for the Information Society" (SMART 2007/0037), study of European Commission, available at:http://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037, the whole document.

[60] Sterling, Adrian, "World Copyright Law"; Sweet & Maxwell; 2008; p. 547: "no rules are laid down in the Directive as to what constitutes actual knowledge, or how the service providers might obtain it".

[61] This was decided e.g. in judgment of the Court of Justice of European Union of 27 September 1988.; *Belgian State v René Humbel and Marie-Thérèse Edel*.; Case 263/86 and in the judgment of the European Court of Justice of 7 December 1993; *Stephan Max Wirth v Landeshauptstadt Hannover*; Case C-109/92.

[62] The catalogue was created in recital 19 of Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.

of an e-government approach and monitoring the usage of new technologies in higher education, a negative answer to the question will create a difficult legal situation where some institutions will face a higher threshold of internet liability.

It is already well established in CJEU jurisprudence that "remuneration" does not have to be directly related to the user – income can come e.g. from commercials.[63]The controversy can be caused by a business model of hosting providers such as Wikipedia (online wiki) or Flickr (photo-sharing site). Do they "normally" provide for remuneration? The answer is clear – as examples of more and more popular "freemium" online model[64] they do not benefit economically, neither from users' fees nor commercials. Does this mean that they are excluded from benefitting from the liability regime provided in the E-Commerce directive? The question will probably soon be answered by CJEU.

1.2.4.2. Passiveness

The other very controversial notion is "passiveness" – to benefit for legislative safe harbour any ISP has to remain passive. The concern what "passive" means was tackled by CJEU.

The first decision worth noticing is *Louis Vuitton v. Google France*[65] which concerns Google Adwords - a commercial system operating on very simple business model – once you pay for certain word, your ads will be shown alongside with Google search related to this word. Louis

[63] Judgment of the Court of Justice of European Union of 26 April 1988, *Bond van Adverteerders and others v The Netherlands State*, case 352/85.
[64] Van Eecke, Patrick and Maarten Truyens "Liability of online intermediaries" in: "Legal analysis of a Single Market for the Information Society" (SMART 2007/0037), study of European Commission, available at:http://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037, p.12.
[65]Judgment of the Court of Justice of European Union of 23 March 2010; *Google France SARL and Google Inc.v Louis Vuitton Malletier, SA and Others*; Joined Cases C-236/08 to C-238/08.

Vuitton and other companies sued Google for trademark infringement – competing companies bought words related to original ones and therefore were promoted next to Google search related to e.g. new Louis Vuitton bag.

The court decided that Google cannot be held liable since Google Adwords is an automatic system and can benefit from protection under article 14 (contrary to the decision of the French Court in first instance). Any service provider (even referencing) cannot be held liable if its role is passive *"*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".[66] The decision was warmly welcomed by the Internet environment as reassuring safe harbour scheme,[67] but also is a warning signal for Google and other worldwide companies, that their role has to remain purely passive. Of course, the decision is not earth-shattering, but gives the possibility of extending the scope of subjects covered by article 14 of the E-Commerce directive.

The Court had a chance to elaborate on notion of "passiveness" also in *E-Bay v. L'Oreal case*.[68] E-Bay, as one of the main online marketing platform, was sued by L'Oreal in the United Kingdom[69] for trademark infringement – it was (and still is) possible to buy on e-Bay the counterfeits with L-Oreal logo, not-for-sale cosmetics samples or original products without proper packing.

[66] Para 114.
[67] E.g. Doobay , Dhana; "Google AdWords benefits from E-Commerce hosting defence", available at: http://www.ashurst.com/publication-item.aspx?id_Content=5260, last accessed on 15 November 2013.
[68] Judgment of the Court of Justice of European Union of 12 July 2011; *L'Oréal SA and Others v eBay International AG and Others*; C-324/09.
[69] And not only – the proceedings were initiated in many other European countries, see: "L'Oréal v eBay – clarification of online marketplace operators' liability for its users' trade mark infringement", available at: http://www.herbertsmithfreehills.com/-/media/HS/T2909111725.pdf, last accessed on 15 November 2013.

Comparing to the first discussed case, the court did not decide that E-Bay generally plays "passive role", but distinguish mere providing of sale platform from promoting and optimizing the presentation of products (in such situations eBay cannot benefit from liability exemption).[70] Moreover, the Court introduce the threshold of what "diligent economic operator should have realized"[71] as a situation in which article 14 cannot be applied. Unfortunately, the court left new standard without further elaboration what it actually means and only stated that eBay's Verified Rights Owner (VeRO) notification scheme is not sufficient to prevent trademark infringements.

The case is perceived by many as a "move towards greater accountability"[72] shows that an ISP can be liable not only once it plays active role, but also in a situation of a negligent failure. Therefore the scope of ISP legislative safe harbour was limited comparing to previous, very broad interpretations of circumstances when it can be applied.

1.2.4.3. Other controversies

Moreover, the language used in Article 14 is controversial. The hosting service, according to the definition provided in article 14, "consists of the storage of information provided by a recipient of the service". Such a definition is a ground for distinguishing hosting providers from active content providers – entities such as online magazines involved in publishing their own content (and therefore they do not benefit from liability regime). Such a strict approach was easy to apply a while ago, but nowadays with web 2.0 services with very

[70] Para 123.
[71] Para 120.
[72] James, Steven, "L'Oréal v eBay & the growing accountability of e-operators" , *e-commerce law & policy*, 2011, volume 13 issue 9, p. 4.

developed packages of services it is tricky to evaluate which ISP provides only hosting and which content – the line became blurry.

The decision as to what extent service "consists of the storage" (majority, all, any?) was left for national courts and it results in interpretation inconsistency, even within one jurisdiction. Comparing only decisions of the Court of Paris shows that the catalogue of ISPs covered by article 14 is very discretional. The same court decided that MySpace is not covered by the E-Commerce directive (MySpace was called an editor of the music content hosted on the webpage),[73] while YouTube can rely on safe harbour under article 14 (and other options of the portal were not taken by the court into consideration).[74] Any Internet user knows how similar those portals are and cannot understand what makes only one of them recognized as a hosting provider, according to the Court's rulings.

There is no doubt that the E-Commerce directive was introduced with the intent to protect further development of innovation in the e-commerce sphere. Unfortunately, providing liability regime with open for interpretation notions and without clear application procedures makes efforts fairly unproductive.

1.3. An overview of national laws implementing the ISP legislative safe harbour provision

Addressing the issue on UE level is one issue, implementing in national legal systems is another – the question to be addressed in the next section is if on both levels the aims

[73]Paris Tribunal of First Instance (emergency proceedings), *Lambert J-Y dit Lafesse v Myspace Inc* 22 June 2007.
[74]Paris Tribunal – Grand Chamber, *Bayard Presse v. YouTube LLC*, 10 July 2009.

of regulation were achieved and how sufficiently national transposing laws in member states secure fundamental freedoms and create certain legal framework.

The E-Commerce Directive is legally binding on the effect, but methods and forms of achieving its aims were left to the member states.[75] Therefore all provisions to be enforceable require transposition and implementation into member states' legal systems. 12 out of 15 member stated managed to transpose the directive by the formal deadline of 17 January 2002.[76] This part shows how ISP legislative safe harbour provisions were transposed into legislations on the national level. What's interesting is that many countries transposed quasi-literally section 4 of the directive,[77] but still the outcome of implementation is perceived by many as controversial.[78]

1.3.1. Remarks on general trends in the European Union

The notification, as a precondition of knowledge, is particularly important for the understanding and operating of the whole safe harbour system. There are countries where a mere letter or an e-mail are sufficient to initiate the whole procedure. The majority of countries do not

[75] Margot Horspool and Matthew Humpreys; "European Union law"; Oxford University Press, 2010; p. 114.
[76] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee - First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce); COM/2003/0702; p.6.
[77] With few exceptions, such as Germany – in the Telemedia Act (Telemediengesetz, BGBl. I S. 179, 26 February 2007) the term "knowledge" instead of "factual knowledge is used, in Portugal (in para 16 of Decreto-Lei - Law-Decree no 7/2004 of 7 January 2004 on e-commerce) the safe harbour cannot be applied when a ISP should be aware of the illegal content.
[78] Christou, George "The EU and Internet Commerce Regulation" in: George Christou and Seamus Simpson "The new electronic marketplace : European governance strategies in a globalising economy"; Edward Elgar Publishing Limited 2007, p. 119.

have formal notification procedure,[79] although some introduced statutory criteria.[80] The way notice and take down procedure is established also varies. In France and Lithuania the procedure is optional, whereas in Hungary and Finland its scope is limited to IP infringements.[81] In Spain[82] and Italy[83] the notice must be confirmed by a court or an administrative authority to be binding for an ISP, although still the situation of the content author is not regulated (if he should be notified, given any way to appeal decision etc.).

There are countries, such as the United Kingdom, where the requirements for notification were established as guidelines for courts, not implementation measures. Regulation 22[84] provides that any court should take into consideration all relevant circumstances, such as a known name of a notice sender and the accuracy of information provided in the notice.[85]

Disputable is also an issue what "acting expeditiously" means. In France the assessment is done on case-by-case basis and can mean few hours to few days, depending on the nature of infringing content.[86] In Italy an ISP is obliged to remove child pornography within 6 hours

[79] E.g. Denmark or Germany.
[80] E.g. Portugal.
[81] According to article 15 of Finnish Law (Act on provision of information society services, 458/2002, 5 June 2002), the situation varies depending on what kind of infringement ISP have to face – in situation of "clear criminal offences" action has to be taken promptly, in IP cases only notification from party claiming infringement places the duty to take action – in other cases the court decision is necessary
[82] Article 16.1(b) of the Spanish Law of Information Society Services and Electronic Commerce (Ley de Servicios de la Sociedad de la Información y de ComercioElectrónico, 34/2002, 11 July 2002).
[83] Article 14 of Legislative Decree No 70 of 9 April 2003 (DecretoLegislativo 9 aprile 2003, n. 70.
[84] Part of The Electronic Commerce (EC Directive) Regulations 2002, SI 2002/2013.
[85] See Queen's Bench Division (UK), *Bunt v. Tilley & Others* [2006] EWHC 407 (QB), Great Britain – British Telecom was not held liable for defamatory content in the situation when the notice did not contain information on illegal nature of the content nor specific location of the content – Mr Justice Eady stated : "I am also prepared to hold as a matter of law that an ISP which performs no more than a passive role in facilitating positing on the internet cannot be deemed to be publisher at common law" (para 36).
[86] Vaciago, Giuseppe and Silva Ramalho "The Variety of ISP Liaiblities in the EU Member states", *Computer Law Review International* 2/2013, p.34.

after the content was flagged up.[87] The legislator remained silent about the other situations when notice and take down is implemented.

Different actions are expected to be taken by ISPs in various legislations. Some countries, such as Finland[88] and Lithuania[89] oblige ISPs to block access to potentially illegal content, without obligation to take down the publication. A different approach was introduced in the Slovak Republic, where ISPs has to remove content. In Belgium ISPs have not only block or remove the content, but also notice the competent authority about allegedly infringing content.[90]

Many other differences (concerning the legal qualification of the host provider, understanding of actual knowledge relationship to press law) can be noticed across EU member states. It is a consequence of very vague and not-precise Directive – many issues were left to be decided by national legislations and in result these matters were not legislated at all – most countries decided for verbatim legislation of provisions.[91]I will now elaborate more on the issue who the subject is regulating, how the notice and take down procedure looks due to the relevance of the issue for human rights analysis.

[87]Ministerial Decree (Italy) on network blocking of child pornography website, 8 January 2007.
[88] Section 15 of Act on provision of information society services, 458/2002, 5 June 2002, unofficial translation by Ministry of Justice available at: http://www.finlex.fi/en/laki/kaannokset/2002/en20020458.pdf.
[89] Article 14 of Law on Information Society Services of the Republic of Lithuania, 25 May 2006, No. X-614.
[90] Belgian E-Commerce Act of 11 March 2003, article 21§2.
[91] Vaciago, Giuseppe and Silva Ramalho "The Variety of ISP Liaiblities in the EU Member states", *Computer Law Review International* 2/2013, p.37.

1.3.2. Notice and take down procedure: state-, self- and co-regulation

The notion of "notice and take down" it is not introduced by the Directive, is not even mentioned literally in the text. Nevertheless, in practise this is usually the way how directive requirement that "the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information"[92] is implemented by ISPs. The Directive encourages self- and co-regulations of ISPs' approaches to illegal content.[93] Even though there is no EU agreement on these two notions, it is possible to describe some examples of regulations provided at national and company level.

Finland is an example of a state that decided to regulate notice and take down procedure in a codified way.[94]According to the International Data Corporation's Information Society Index,[95] Finland is one of the leading actors in the ICT sector. The Directive was transposed in the Act on the Provision of Information Society Services.[96] While discussing transposition of article 14, contrary to other member states, constitutional concerns were raised.[97] The original governmental proposal of the notice and take down procedure was claimed to be violating freedom of expression provided by section 12 of the Finnish Constitution. While redrafting provisions on notice and take down two opposite approaches clash (ISPs opted for court orders as a legal base for any action against content of webpages, copyright holders favoured a self-regulatory model and leaving broad scope of discretion for ISPs). In the end a compromise

[92] Article 14 of the E-Commerce Directive.
[93] Article 16 of the directive puts an obligation on both the Commission and member states to encourage self and co-regulation to achieve better outcomes of directive implementation.
[94] Other examples might be Lithuania and Hungary.
[95] Database available at: *www.idc.com/groups/isi/main.html*, accessed on 14 April 2013.
[96] Act on provision of information society services, 458/2002, 5 June 2002.
[97]Christou, George and Semaus Simpson; "The new electronic marketplace: European governance strategies in a globalizing economy"; Edward Elgar Publishing Limited, 2007; p. 122.

was achieved and the regulation similar to the American was introduced: notice and take down must be authorized by a court (except copyrights cases where a reliable notification is enough to take down the content).

In many EU countries the formal requirements of the procedure were left in ISPs hands (so called self-regulation). In Austria, the Austrian Internet Service Providers Association[98] introduced a code of conduct specifying the requirement of notice and take down procedure. The code is binding for all members of the Associations and covers all possible situations in which safe harbour provision can be used (both criminal and civil liability). The code focuses on the relation between right holders and ISPs and does not mention the role of content creators, not providing any counter-notice procedure.

A self-regulation approach is also popular in the UK, with the leading example of the Internet Watch Foundation[99] – the NGO that makes efforts to restrict access to child pornography and materials on racial hatred. Many ISPs are members of the Foundations and agreed on prompt actions after receiving notification about illegal content from the foundation.

Some countries decided to introduce a co-regulation approach to notice and take down. The Federal Computer Crime Unit[100] is a body created in Belgium based on agreement of the biggest ISPs' organization and Ministries of Justice from 1999. All possibly illegal content has to be notified to the Crime Unit which makes a decision on further actions (informing prosecution, taking down, blocking access).

[98] More information available at the webpage of the Austrian Internet Service Providers Association: www.ispa.at.
[99] More information available at Foundation's page: https://www.iwf.org.uk/.
[100] More information available at: https://www.ecops.be/webforms/Default.aspx?Lang=EN.

The above examples show that national legislations implementing the E-Commerce Directive varies significantly. The situation results from very general regulations of the directive and conscious decision to leave some ISP liability aspects to member states discretion. Therefore I do not find the E-Commerce directive a very effective legislative measure that creates common e-market – in practice still discrepancies are significant.

1.3.3. Conclusions

The European Union, compared to US and very detailed regulation provided in Digital Millennium Copyright Act, decided to approach the issue of ISP secondary liability in a more flexible way.[101] But leaving such a broad discretion in states' hands results in creating a situation, when it is very difficult to assess when ISPs can be held liable.[102] On the one hand there is no obligation to monitor, on the other what factual knowledge means is disputable.

Moreover, the EU seems to forget that the Internet and sharing information cannot be possible without all types of providers mentioned in the E-Commerce directive, but not only. Taking into account the rapid network development, there are many e-services with complicated legal characteristics. The question is, how to qualify cloud computing, web 2.0 services and web services, wikis, or content sharing services? Other controversies arise around the issue o

[101] Smith, Emerald; "Lord of the Files: International Secondary Liability for Internet Service Providers"; *Washington & Lee Law Review* 68(3), 2011, p.1588.

[102] Litwiński, Paweł; „Zasady odpowiedzialności pośrednikow w dostarczaniu informacji w internecie" [Rules of liability of ISP]; *Monitor Prawniczy* 24/2002, p.7.

f hyperlinks, location tools and content aggregators?[103] We see that the E-Commerce Directive addresses the issue of ISP liability, but certainly does not create a complex legal framework.

The legal situation in the EU might by summed up by words of Kim Walker: "The issue of when a host was liable has been getting a bit vague and some hosts in Europe have been getting a little bit upset".[104] Such an uncertain and disputable situation related to assessment of business legal framework makes the issue of ISP secondary liability very controversial from a human rights perspective. All question marks also influence human rights protection – this is the main assumption of the next chapter.

[103] That was the subject of 2010 Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce; available at: http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.

[104] Pfanner, Eric; "YouTube can't be liable on copyright, Spain says", *New York Times*; published on 23 September 2010; available at: http://www.nytimes.com/2010/09/24/technology/24google.html, last accessed on 13 November 2013.

CHAPTER 2 – ISP SECONDARY LIABILITY– APPLICABLE HUMAN RIGHTS STANDARDS

Having elaborated on E-Commerce Directive, including the mechanism through which it is implemented in national legal systems and the reasoning behind choosing such a liability regime, chapter 2 explores the inroads of ISP liability to human rights. It can be perceived as a lead-in to a more comprehensive evaluation of ISP liability from the human rights perspective in chapter 4.

The initial statement of the thesis is that in the contemporary era, the Internet is the most easily-accessible platform for publications and sharing opinions. I would even make the statement that it is the most important platform in which the right to freedom of expression is both exercised and violated.[105]However, it is also an environment where freedom of expression is often present in a way that creates the situation of human rights clashes (for example, in the case of slander and defamation, when freedom of expression must be balanced with the protection of reputation). Chapter 2 provides an overview of issues necessary for better understanding the significance of human rights for ISP secondary liability.

The chapter is divided into three parts. Part I mostly elaborates on substantive guarantees for freedom of expression. It also addresses two points related to slander and defamation on the Internet relevant from a human rights perspective: the threat for ordinary users to be accused of defamation is higher online than when they use regular means of communication and the

[105] Solove, Daniel J. "The Future of Reputation: Gossip, Rumour, and Privacy on the Internet", New Haven: Yale University Press, 2007, p.76.

victims of defamatory statements encounter various challenges in pursuing any legal action. An understanding of these two issues is crucial for further research for two reasons. First of all, on the Internet, due to the anonymity of users, it is sometimes impossible to discover the identity of an author of an abusive publication; therefore, the regime of secondary liability was established.[106] Secondly, defamation law in the CoE context might be used as grounds for limiting freedom of expression (as the right of others).[107]

Part II focuses on the question of guarantee rights for realizing freedom of expression online, which should be applied also to the notice and take down procedure. More specifically, it examines the guarantee rights established by the European Court of Human Rights (ECtHR) in the cases related to freedom of expression. The final part shows how the ECtHR directly addresses the issue of ISP liability in the controversial and recent decision of the First Chamber in Delfi v Estonia. The evaluation of the case makes it possible to depict the challenge of the issue we are facing and how further discussion and developments related to notice and take down are required.

The chapter refers to international standards with a special focus on CoE and ECtHR jurisdiction. It argues that ISP liability is a very complex issue from a human rights perspective and that it is a very appropriate moment to deal with the issue more closely on the international forum, since inconsistency and legal uncertainty can cause harm, not only for the Internet as a business model, but above all to freedom of expression.

[106] Solove, Daniel J., "The Future of Reputation: Gossip, Rumour, and Privacy on the Internet", New Haven: Yale University Press, 2007, p.67.
[107] Milo, Dario, "Defamation and Freedom of Speech. Oxford", UK: Oxford University Press, 2008, p.113-114.

2.1. ISP secondary liability and human rights- substantive guarantees

This part of the chapter addresses two questions. Firstly, does substantive protection of freedom of expression on the Internet vary from the protection that is exercised in the non-virtual world. The predominant understanding is that the scope of the right has not changed and the expression still protects the threshold "hold, receive and impart".[108] Some authors claim that the only thing that has changed is the technological context.[109] Examination of the standards applicable for the freedom of expression online, taking into consideration the aims of the freedom and the obstacles faced by traditional way of exercising freedom of expression, demonstrates that the development of the Internet helps to extend the scope of the right and makes it more accessible.

Secondly, since the thesis deals with ISP secondary liability in defamation cases, this part of the chapter also addresses the issue of defamation and slander online from substantive perspective, character and possible challenges faced by freedom of expression defenders.

[108] Gisbert, Rafael Busto, "The right to freedom of expression", in: Javier García Roca, Pablo Santolaya (eds.), "Europe of rights : a compendium on the European Convention of Human Rights", Martinus Nijhoff Publishers, p.372.
[109] Balkin, Jack M., "The Future of Free Expression in a Digital Age", Faculty Scholarship Series, 2009, p. 429.

2.1.1 The Internet as a new environment of exercising freedom of expression – specific and standards applicable.

Without a doubt, the evaluation of the Internet fosters the process of individualizing freedom of expression.[110]From the very beginning, it was claimed that individuals mostly have the freedom to hold opinions, whereas mass media exercise the right to disseminate information. In the contemporary times, this borderline is not so significant and as easy to establish as it used to be – some bloggers have more readers than popular daily newspapers. Moreover, the Internet is a very inclusive tool,[111] enabling previously marginalized citizens and viewpoints to gain access to very broad audience.

Many authors became involved in a critical discussion over the catalogue of aims of the freedom of expression. The most comprehensive listing[112] combines aims related to both individual self-fulfilment and development of society as a whole. The first group focuses on self-expression and the exchanging of ideas with others in order to form own opinions. Access to the Internet makes it possible for many people, even those who may not know each other, to get involved in exchanging opinions. Internet content, due to its open and global character, is usually not a subject of any censorship,[113]making it possible for anyone to gain access and familiarize themselves with various, sometimes even controversial, ideas. Moreover, rather than one-way communication, the Internet promotes dialogue (through comments, chat rooms), which likely

[110] Weber, Rolf, "ICT Policies Favouring Human Rights" in: John Lannon and Edward Halpin (eds.) "Human Rights and Information Communication Technologies: Trends and Consequences of Use", IGI Global, July 2012, p.26.
[111] Gilton, Isabel, "When everything has a price", *Guardian*, 27 August 1996.
[112] Cucereanu, Dragos, "Aspects of Regulating Freedom of Expression on the Internet" , *School of Human Rights Research Series*, V. 27: Antwerpen : Intersentia, 2008, p.166-168.
[113] With exception of totalitarian countries that make attempts to monitor and regulate the content of the Internet

contributes to a more comprehensive exercise of the right to freedom of expression by individuals.

The aims of freedom of expression related to society focus on participation in public life, monitoring of authorities and mechanisms for protecting and exercising other rights (such as freedom of religion). The Internet is an easy-to-use and widely accessible tool for citizens to communicate with the authorities; all various measures of so called e-government[114] enhance the "social watch dogs" role. In some countries (for example in Estonia) the Internet plays an important role in the process of operation of the administration. The Internet, as not under governmental control, is also an environment for establishing and facilitating social campaigns devoted to achieving certain changes – it makes cooperation among people easier and faster.

The limits of freedom of expression might be divided into two main groups: technological and regulatory. The Internet enhances freedom of expression by undermining the significance of both. The global network makes it possible to communicate with people regardless of the distance between individuals. Furthermore, not only voice, but also images can be transmitted. The Internet does not require communication to take place in "real time". Its "asynchronous character"[115] enables storing messages and access to them in the time suitable.

What is also essential is that the content online might be produced by anyone with minimal technical skills, without any journalistic training. It is also a very cost-effective way of communicating ideas to mass audiences, particularly compared to newspapers or TV. The previous widely available tools were limited in scope of dissemination.[116] Additionally,

[114] The Information for Development Program , "The e- Government Handbook For Developing Countries", available at: http://www.infodev.org/en/Publication.16.html, last accessed on 8 November 2013.
[115] Jakubowicz, Karol, "Media and Democracy", Council of Europe Publishing, Strasbourg, 1998, p.25.
[116] Cucereanu, Dragos, "Aspects of Regulating Freedom of Expression on the Internet" , *School of Human Rights Research Series*, V. 27: Antwerpen : Intersentia, 2008, p. 139.

the Internet provides all types of content, whereas TV and radio broadcaster grant access to previously selected and usually edited materials.

In the history of fundamental rights, various types of regulations imposed by authorities on freedom of expression can be defined: content, context, and form. Some of them are still applicable in the case of the Internet, especially regulations based on reasonable prerequisites and regulated by law (as in the case of criminalizing child pornographic content). On the other hand, sometimes governments establish some limitations in order to avoid criticism – in such cases the Internet and technological development might help to overcome such regulations and create different tools and measures of citizens' communication.

The last comment issued by Human Right Committee regards article 19, which refers to freedom of opinion and expression.[117] The experts emphasize that the Internet has "substantially changed communication practices around the world".[118] The countries are encouraged to adopt such legislative measures that are the most suitable for the most recent technological developments. Restrictions on freedom of expression online, access to networks, ISP activity and search engines are permissible only when in accordance with limitation provisions from the International Covenant on Civil and Political Rights. Not much attention is devoted to online freedom of expression in the comment, but it is made clear that all standards generally applicable for the freedom of expression should be also binding for the Internet.

The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, from 2011, focuses on the Internet.[119]

[117] Human Rights Committee, "General comment No. 34. Article 19: Freedoms of opinion and expression", CCPR/C/GC/34, 12 September 2011, available at: http://www2.ohchr.org/english/bodies/hrc/comments.htm, last accessed on 8 November 2013.
[118] Comment no. 15.
[119] Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue", A/HRC/17/27, 16 May 2011, available at

He believes that the Internet is now the most powerful tool for exercising freedom of expression and emphasizes that this is the case not only because of the free access to uncensored content, but also because of the availability of infrastructure (which is outside the scope of the thesis). He enumerates imposing disproportionate secondary liability[120] among other threats for free Internet as: "arbitrary blocking or filtering of content; criminalization of legitimate expression; disconnecting users from Internet access, including on the basis of intellectual property rights law; cyber-attacks; and inadequate protection of the right to privacy and data protection".

The report raises a very important issue that regarding a set of actors involved in ISP liability: not only the service provider and the Internet user, but also the state. Human rights traditionally have vertical character, regulating states' behaviour towards individuals.[121] This is based on the assumption that non-state actors are not party to international human rights treaties and therefore they cannot be held liable for any violation. Currently, an increasing number of scholars are demanding a change in this approach, with the demand that some level of accountability be placed on international organizations or even cooperation, since they have already become nearly equal partners for countries in many areas of public international law.[122] Such a shift would also be an adequate response for such divisive issues as outsourcing, privatization, and land-grabbing. Such an approach for many will be just a trivialization of human rights; for others it is essential that human rights should cover current challenges.[123] Unfortunately, the ECtHR still has not taken any further steps in extending the list of actors

http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf , last accessed on 9 November 2013.

[120] Paras 44-48.

[121] Clapham, Andrew, "Human Rights Obligations of Non-State Actors", Oxford: Oxford University Press, 2006, pp. 46-53.

[122] Ziemele, Ineta, " Expanding the horizons of human rights law", The Raoul Wallenberg Institute new authors' series, Leiden, 2005, p.31.

[123] Clapham, Andrew, "Human Rights Obligations of Non-State Actors", Oxford: Oxford University Press, 2006, p. 103.

involved in human rights protection. *Appleby and others v. United Kingdom* might be an example – the ECtHR stated that the private owner of the shopping mall had the right to limit freedom of expression of the costumers and reiterated that human rights are part of the public domain, not private.[124] Nevertheless the ECtHR, in various cases discussed afterwards, created the concept of states' positive obligation which requires states to create the appropriate legislative framework to reinforce freedom of expression.

The Internet provides a situation in which private actors – ISPs – have gained control over individual freedoms, although they may still not necessarily be held accountable for violations. The rapporteur recommends that ISPs take action that encroaches on fundamental freedoms only after judicial proceedings – without doubt the regulation of secondary liability in the E-Commerce directive is in opposition to such recommendation. Generally the approach of making an ISP liable for third party content published on its servers is criticized as having a negative effect regarding freedom of expression for regular users – in an effort to comply with local laws and avoid liability, ISPs may be overly eager to take down content.

Ultimately, the Internet is not only another mean of communication, but it also has a visible impact on the freedom of expression, including its accessibility and scope. Low costs of internet, lack of prerequisites, and anonymity encourage more people to become engaged in exchanging opinions.[125] Therefore it is essential to protect the Internet as an environment in which free speech can be exercised. The hosting ISPs should be very careful in their

[124] The critique of the case: Gerstenberg, Oliver H., " What Constitutions Can Do (but Courts Sometimes Don't): Property, Speech, and the Influence of Constitutional Norms on Private Law", *Canadian Journal of Law and Jurisprudence*, Vol. 17, No. 1, January 2004, pp. 61-81.

[125] Organization for Security and Co-operation in Europe The Representative on Freedom of the Media, "Amsterdam Recommendations on Freedom of the Media and the Internet" from 14 June 2003, available at: http://www.osce.org/fom/13854, last accessed on 8 November 2013.

interventions in order to keep any limits in the right to freedom of expression within acceptable boundaries.

2.1.2. Limitation of freedom of expression – test of compliance with standards established by the European Court of Human Rights and ISP secondary liability remarks.

Freedom of expression, even as substantial as it is for democratic societies, is not unlimited. There are situations where two freedoms clash; consequently, a decision is necessary regarding what to do about the relevant encroachment. Since the thesis focuses on the clash of freedom of expression and the right to reputation in defamation cases, it is essential to recall the conditions under which freedom of expression might be limited. The research is conducted within European legal scope, therefore the limits of the freedom are established in decisions of the ECtHR elaborating on article 10 § 2 of the European Convention on Human Rights (ECHR):

"The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

To assess the legal framework of ISP secondary liability from a human rights perspective, an evaluation through the so-called three steps test by the ECtHR is indispensable.[126] Of course, a case of interference is a prerequisite for application of the test. It can be achieved both by some direct measures (as prior restrains, injunctions, criminal and civil liability imposed on the author)

[126] Cucereanu, Dragos, "Aspects of Regulating Freedom of Expression on the Internet" , *School of Human Rights Research Series*, V. 27: Antwerpen : Intersentia, 2008, p. 13.

and actions resulting in negative effects.[127] As introduced in chapter 1, the result of ISP secondary liability is equal to an interference, but not in the direct way (non-authorities parties take action violating freedom of expression). Nevertheless, the interference of ISPs into content online via notice and take down procedure being prescribed by law is an interference credited for the state which created the regulation.

The three-step-test that determines if an infringement into the right to freedom of expression is legitimate requires first that the state's interference into freedom of expression must be prescribed by law. The name of the legislative act is irrelevant; the features that should be assessed are its accessibility and foreseeability.[128] The accessibility means both the form that is "accessible" in a technical way, as well as being "accessible" in terms of plain language so that ordinary citizens can understand it – both form and language matter. The foreseeability requires such precision that allows citizens to regulate their behaviour in order to act according to the law. Of course, a "certain degree of flexibility" is permissible.[129] The analyses of the ECtHR jurisdiction shows that usually the Court does not concern the condition of being "provided by law" as a ground for violation of rights and concedes a high level of legitimacy in CoE countries.

The second part of this test requires that any limitation be in pursuit of a legitimate aim – there are six aims enumerated which can limit the right to freedom of expression, namely: national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for

[127] Ovey, Clare, Robin C. A. White and Francis Geoffrey Jacobs (eds.), "The European Convention on Human Rights", Oxford : Oxford University Press, 2006, p.277 at seq.
[128] European Court of Human Rights, *Malone v. the United Kingdom*, application no. 8691/79, judgment of 2 August 1984.
[129] European Court of Human Rights, *Goodwin v. the United Kingdom*, application no. 28957/95, judgment of 11 July 2002, para.33.

preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. The Court has approached the Convention as a "living instrument," making it possible to extend the catalogue through aim-oriented interpretation.[130] As the paper focuses on ISP secondary liability in defamation cases, the only aim excusing limitation of freedom of expression of users can be the "protection of reputation or rights of others" with regard to the right to privacy.

The last, and the most controversial and scrutinized part of the test is necessity in a democratic society. The last requirement, due to its ambiguity, has shown disagreement among scholars[131]and in case-law. For the three steps test, necessity means the existence of "pressing social need"[132], relevant and sufficient reasoning beyond limitation and proportionality of measures used to achieve the aim. The pressing social need implies the gravity of the need and also the margin of appreciation left for countries which are the best suitable to assess which aims and values are desired by the certain society. The need behind ISP secondary liability is to avoidthe creation of a legal gap where no one can be held liable for defamation statements online. The scheme provides that the author of a publication cannot be identified and if ISPs do not follow the notice and take action procedure, they will be liable for the statement. This solution results in situation in which the victim of defamation might gain remedy, or at least the defamatory statement are blocked.

The "relevant and sufficient reason" part of the test is a link between pressing need and limitation – the ECtHR emphasizes that national courts and authorities are obliged to give

[130] Dijk, P. and Yutaka Arai, "Theory and Practice of the European Convention on Human Rights", Antwerpen: Intersentia, 2006, p. 771.
[131]Harris, O'Boyle & Warbrick, "Law of the European Convention on Human Right", Oxford University Press, 2009, p.361.
[132] European Court of Human Rights, *The Sunday Times v. The United Kingdom*, application No. 6538/74, judgment of 26 April 1979.

sufficient concerns about freedom of expression implication of their infringements and have to provide sufficient reasons for limitation that might be evaluated by public opinion.

The proportionality requirement again is constructed from different factors, as suitability, balancing of measures and outcome and lack of less restrictive means.[133] Suitability means "reviewing whether the restriction is appropriate to achieve the aim pursued".[134] Suitability should be assessed on the basis of factual knowledge, research and previous experiences. Without a doubt, ISP secondary liability facilitates and enhances protection of reputation by creating a legal system that enables the victims of defamation claims to exercise their rights. The national authorities should also consider if there is no less restrictive measure available to achieve the same aim – any interference into human rights should be as minimal as possible. Human rights, as a core value of any democratic society, should be aimed at protecting as much as possible. Therefore, usually civil liability is perceived as less intrusive as compared to criminal measures. And measures targeted to specific social groups are usually more appreciate than those covering the entire society. The last step of assessing legitimacy of state interference is balancing between means and results – in other words comparison of benefits and costs of any limitation. While elaborating on ISP secondary liability, the social costs might be very high – with a negative effect on the Internet and private censorship of content, there may be diminished trust of society in the global network. Therefore, this aspect, as well as prescribing by law are the most scrutinized in the next chapters.

[133] European Court of Human Rights, *Brogan and others v. the United Kingdom*, application no. 11209/84; 11234/84; 11266/84; 11386/85, judgment of 29 November 1988.
[134] Bosma, Heleen, "Freedom of Expression in England and Under the ECHR" in Heleen Bosma (ed.) "Search of a Common Ground - a Foundation for the Application of the Human Rights Act 1998 in English Law", Antwerpen: Intersentia/Hart, 2000, p. 139.

2.1.3. The problem of slander and defamation on the internet

Protections against slander and defamation are perceived as measures to protect personal reputation. The legislation on these libels vary from country to country, with still existing penalization in some of them, even European.[135]The protection of reputation, compared to the freedom of expression, in the Internet environment gains new scope and faces new challenges.[136]

The Internet is a "defamation-friendly" environment due to its specific and international scope. The author of the publication cannot fully monitor and control the ways and places where his statement are used – therefore even defamatory remark made in private e-mail may become easily available for everyone – the speed of transmission information is unprecedented. Moreover, the Internet is an international network which results in application of various jurisdiction to the same content, on the basis of various factors, as the place of posting or place of access (which can be literally anywhere).[137] The author of seemingly defamatory-proof statement from one country might end up being sued for defamation in another, with more strict liability system.[138]

The choice of jurisdiction and law is not only a challenge for a person posting some content online, but also for the individual seeking redress for defamatory statements. Moreover, there is a question with regard to the liability of an ISP, which does not provide any defamatory

[135]Ovey, Clare, Robin C. A. White and Francis Geoffrey Jacobs. Jacobs and White,the European Convention on Human Rights: Oxford : Oxford University Press, 2006, p.254.
[136] Only few countries have separate legislations on defamation online (e.g. UK Defamation Act 1996), usually the standard rules are applicable.
[137] Edwards, Lilian, "Defamation and the Internet" in: Lilian Edwards and Charlotte Waelde (eds.) "Law and the Internet : Regulating Cyberspace", Oxford : Hart Publishing, 1997, p. 184.
[138] So called „libel tourism" - Taylor, Daniel C., "Libel Tourism: Protecting Authors and Preserving Comity", 99 *Georgetown Law Journal*189, 2010-2011.

content itself, but rather serves as a platform on which such an opinion can be published. In an era of widespread use of the Internet and unsubscribed access to most blog platforms and forums, it is technically impossible to monitor content before it is published.[139] Moreover, defamatory statements are not characteristic for specific groups of content. The Internet facilitates the grouping of people with similar interests, sometimes illegal as piracy or pornography – such situations are easy to evaluate from legal meaning even for non-lawyers. The situation is totally different in the case of defamation - it might come in the form of acomment under a blog post, a poem, a remark on a newspaper article, an answer on a forum – virtually everything – it makes hosting ISPs commercial activity very risky.

The secondary liability is claimed to be a compromise between different approaches to the ISP role on the Internet. Of course, once the author of the publication can be identified, he should be sued and liable. The character of the Internet (the servers and the way to access it through non-personalized computers) leads to various situations in which the identification of the user cannot be established – in such cases it is ISP who can be liable. Some authors support broader scope of ISP liability, comparable to newspapers editors and TV broadcaster that having editorial discretion might influence the content.[140] Others support the treatment of ISA as a "common carriers" (as phone companies) emphasizing that the role of ISPs is purely technical without any discretion upon the content.[141] They do not treat the Internet as a medium itself, but more as a network making various media accessible. The secondary liability regime seems to be the only possible agreement between two approaches, although as it is explained

[139] Such tools do exist in case of e.g. child pornography content, but due to very broad concept of defamation (no specific words or pictures can be marked as defamatory themselves) such tools have no use in defamation cases.
[140] Akdeniz, Yaman and Horton Rogers, "Defamation on the Internet" in: Yaman Akdeniz, Clive Walker and David Wall (eds.), "The Internet, Law and Society", Pearson Education Ltd., 2000, p. 301.
[141] Edwards, Lilian, "Defamation and the Internet" in: Lilian Edwards and Charlotte Waelde (eds.) "Law and the Internet : Regulating Cyberspace", Oxford : Hart Publishing, 1997, p. 192.

further in the thesis, EU member states regulations leave room for doubts and critic from human rights perspective. However, such an approach result in unsolved legal status of the ISPs – they neither monitor everything nor nothing.[142] This results in a very case-based and uncertain approach to ISP liability. Total monitoring is certainly impossible, while lack of any guarantees is socially undesirable – but the solution should be in my opinion legislated, without room for commercial discretion and legal unpredictability.

2.2. ISP secondary liability and freedom of expression - procedural guarantees

Back in 1950, when the ECHR was drafted, freedoms were associated mostly with the state obligation not to interfere in certain areas. Since then the ECtHR jurisdiction has developed significantly in the direction of acknowledging that all rights are combined from substantial and procedural guarantees.[143] Nowadays the mere fact of exercising a certain right without measures to access judicial protection or different forms of remedy for violations is meaningless.

2.2.1. Procedural guarantees – introductive remarks

Fifteen years ago, in the mid-1990s, the World Wide Web started to be available for the mass population, and was enthusiastically welcomed as an unrestrained environment in

[142] Newey, Adam, "Freedom of expression: censorship in private hands" in "Liberating Cyberspace : Civil Liberties, Human Rights, and the Internet", Edited by Liberty, London : Pluto Press, 1999, p. 33.
[143] Nunziato, Dawn, "Procedural Protection for Internet Expression, available at: http://www.osce.org/fom/99458, last accessed on 9 November 2013, p. 2.

which the freedom of speech could be exercised.[144] In the beginning of the XXI century, society was aware that this statement was naïve and speech online should be protected to the same extent as the one in traditional media, also by providing procedural guarantees.[145]

The concept of procedural guarantees is a dimension of the broader issue of content of positive obligations, which is a notion specific for human rights discourse in the CoE.[146] Member states are not only obliged in some circumstances to take positive measures to foster and enable people to exercise their rights, but primarily are responsible for guaranteeing effective rights through procedural guarantees. Therefore the states are obliged to create such a legislative framework which gives full effect to a fundamental right, also in the horizontal relationship between private sector actors, such as ISPs and individuals.

2.2.2. Procedural guarantees for realizing freedom of expression under the European Convention on Human Rights.

Guarantee rights are seldom mentioned in the context of the Internet.[147] Nevertheless, even if the ECtHR is usually very reluctant to refer to any positive obligation in the case

[144] Norris, Pippa, "Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide", Cambridge University Press, 2001, pp. 232-33.
[145] Which was reiterate many times by the Court, e.g. in The Times v UK (application no. 3002/03 and 23676/03, judgment of 10 March 2009) para 45, or even by international bodies, such as the special rapporteur for the freedom of expression in the Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet.
[146] Dimitris Xenos, The Positive Obligations of the State under the European Convention of Human Rights, Routledge Research in Human Rights Law. New York: Routledge, 2012. p. 207.
[147] Meryem Mazouki "The guarantee right for realizing the rule of law" in: Jorgensen, Rikke Frank (ed.) "Human Rights in the Global Information Society", Information Revolution and Global Politics series. Cambridge and London: MIT Press, 2006, p. 95.

of freedom of expression,[148] some guarantee rights can be derived from the jurisdiction referring not only to article 10, but also to article 6. This part is devoted to establishing standards of protection – the discussed cases are not related directly to speech online, but the analogy should be applied.

Since the notice and take down procedure is usually triggered in civil liability cases, the understanding and establishment of fair trial guarantees in civil proceeding is crucial. Article 6(1) of the ECHR covers both civil and criminal cases. The provision went through a significant development process due to the ECtHR jurisdiction – for example the right of access to a court, the right to legal aid, or the equality of arms nowadays recognized as a cornerstone of the protection cannot be derived only from literal interpretation of the Convention.[149]

In one of the first cases on civil proceeding standards, *Golder v. U.K.,*[150] a prisoner was not granted permission to communication with his lawyer to ask him to file a civil complaint in a slander case. The Court decided that the human rights guarantees do not only concern ongoing procedure, but even more importantly concern the right to initiate such proceedings – all obstacles in access to courts should be removed. Different interpretation of the provision will contradict and undermine the whole concept of rule of law.

To allow individuals to properly prepare for civil proceedings, they have to be informed about decisions influencing their civil rights. In *De Geouffre de la Pradelle v. France,*[151]the

[148] Clare Ovey, Robin C. A. White, and Francis Geoffrey Jacobs. Jacobs and White, the European Convention on Human Rights. 4th ed. Oxford: Oxford University Press, 2010, p. 449 – examples of cases were states' positive obligation to protect freedom was recognized are *Fuentes Bobo v. Spain* (application no. 39293/98, judgment of 29 February 2000) and *VgT Verein gegen Tierfabriken v. Switzerland* (application no. 24699/94, judgment of 28 June 2001).
[149] Rozakis, Christos, "The Right To A Fair Trial In Civil Cases", *Judicial Studies Institute Journal*, issue 4, 2004, p.7.
[150] European Court of Human Rights, *Golder v. the United Kingdom*, application no, 4451/70, judgment of 21 February 1975.
[151] European Court of Human Rights , *De Geouffre de la Pradelle v. France,* application no. 12964/87, judgment of 13 December 1991.

Court stated that lack of information of an the applicant about the fact that the law decree that concerns his real estate was in violation of fair trial standard – he was deprived of his right to appeal the decree in the prescribed time.

Freedom of speech is not an unlimited right, but any restrictions should be in accordance with article 10(2) of the Convention. The limitation grounds, repeatedly used in defamation cases, is reputation and the rights of individuals.[152] Of course, defamation legislation conviction or liability must not be based on certain grounds, but must also be prescribed by law and be proportionate.

The Court in *Fatullayev v. Azerbaijan*[153] developed the requirements emphasizing that the national authority is obliged to provide evidence for the existence of "pressing social need" in defamatory cases. The applicant was the chief editor of 'Realny Azerbaijan'. He was held criminally liable for defamatory articles published in the newspaper. The Court's main consideration was balancing between freedom of expression and reputation and the proportionality of criminal conviction. It was also an opportunity to elaborate on guarantee rights in defamation cases. The ECtHR underlined that the liability in such cases must be proceeded by "relevant and sufficient" reasons for the court's decision – it was not the situation in the case – the national court failed to prove defamatory character of statement that were the basis for the conviction. Every freedom of expression limitation must be backed up by certain and sufficient legal explanation and reasoning, without understatements. The domestic courts at the national level are required to provide sufficient and relevant reasoning behind defamatory liability also in online cases.

[152] Cucereanu, Dragos, "Aspects of Regulating Freedom of Expression on the Internet" , School of Human Rights Research Series, V. 27: Antwerpen : Intersentia, 2008, p. 70.

[153] European Court of Human Rights, *Fatullayev v. Azerbaijan*, application no 40984/07 , judgment of 22 April 2010, para 100.

2.2.3. "Duty to give reasons"

The Court also interprets the guarantee rights in a way that "duty to give reasons" also exists not only in judicial proceedings. In *Lombardi Vallauri v. Italy,*[154] the applicant, a professor of philosophy, applied for a teaching post at catholic University in Milan (where he was already employed for 20 years). He was not confirmed by the Congregation for Catholic Education (his views were not in accordance with the Catholic Church which could not be accepted in a catholic university) and therefore excluded from further consideration of his candidacy. He initiated civil proceedings, claiming that the University did not provide him with reasons for the decision. His complaint was dismissed. Therefore, Mr. Vallauri decided to bring the application to the ECtHR, claiming that lack of debate and ability to answer the Congregation's opinion deprived him of his freedom of speech.

The Court concluded that lack of adversarial debate is a violation of article 10. Any decision taken by any authorities - not only execution or judiciary bodies but also in this case public law entities–that influence an individual's legal situation ("*personne juridique de droit public*") should be released with the reasoning of the decision in order to allow the individual to disagree with the decision and to initiate eventual court proceedings. The applicant's guarantee rights were infringed upon – he was not able to exercise substantive freedom of expression due to the insufficient procedural framework.

To sum up, freedom of expression according to the ECtHR is guaranteed by both fair civil trial standards and case-established "duty to give reasons" that enables adversarial

[154] European Court of Human Rights, *Lombardi Vallauri v. Italy*, application no. 39128/05, judgment of 20 October 2010.

discussion. A few more examples of guarantee rights, less relevant for substantial discussion, can be mentioned, such as right to reply[155] or freedom from ex post laws.

2.3. Case study: Delfi AS v Estonia[156]

In a previous paper I wrote: "So far the ECtHR did not literally refer to protection of ISPs activity.[157] Nevertheless, it will have the possibility to elaborate on the notice and take down procedure deciding on the pending case *Delfi As v Estonia*. The question is what measures have to be undertaken by the ISPs to prevent liability. Hopefully the decision will be a trigger for member states and afterwards for the EU to change the procedure in how it provides a guarantee of rights for Internet users."[158]

Finally, on 10 October 2013, the ECtHR rendered its historical decision in the first defamatory case assessing the ISP liability – the decision has been deemed as very controversial and unexpected.

2.3.1. Facts of the case

The applicant – Delfi AS – is one of the biggest online news portals in the Baltic states that can be qualified as both a service and content provider (they publish their own articles, as well as user generated content). Any article can be commented on by readers, who have

[155] E.g. European Court of Human Rights, *Melnychnuk v. Ukraine*, application no, 28743/03, judgment of 5 July 2005.
[156] European Court of Human Rights, *Delfi AS v. Estonia*, application no. 64569/09, judgment of 10 October 2013.
[157] Robert Uerpmann-Wittzack, "Principles of International Internet Law", 11 *German Law Journal* 1245-1263, 2010, p. 1250.
[158] The paper was submitted for prof. Sajo's course "Courts in dialogue" in March 2013.

to provide a name (in practice also nicknames work) and optionally an e-mail. Comments are published automatically, without prior review. The company introduced an internal system of notification and any illegal or abusive comments are deleted promptly after receiving such notification. It is also worth noting that the provider makes it clear that they are not liable for user generated content by posting a warning on the webpage: "The Delfi message board is a technical medium allowing users to publish comments. Delfi does not edit comments. An author of a comment is liable for his/her comment."[159]

On 24 January 2006, an article about a contentious ferry company was published. The main owner of the company was mentioned by name and around 20 defamatory comments appeared. He sued the company for liability (without earlier notification) – Delfi removed comments but refused to accept non-pecuniary damages.[160] The Court of first instance - Harju County Court - dismissed the claim and decided that the company benefits from legislative safe harbor provided by the Information Society Services Act[161] and underlined that the comment activity of the users has to be distinguished from the journalistic work of the company.[162]

Afterwards, the decision was reversed by the Court of Appeal. After re-examining the case, Harju County Court changed its approach and treated the company as a publisher, stating that protective measures taken by the company were not sufficient to protect the rights of others and non-pecuniary damages were awarded.[163] The decision was upheld by the Tallinn Court of Appeal.[164]

[159] Paras 7-11.
[160] Paras 12-16.
[161] Information Society Services Act (Estonia) of 14 April 2004, the act implementing the E-Commerce Directive, implementation is almost verbatim.
[162] Para 19.
[163] Paras 20-23.
[164] Paras 24-25.

On 10 June 2009, the Supreme Court dismissed the appeal, but also changed the reasoning of the lower court. The final decision claims that Delfi cannot be perceived as an information society service provider, as understood in the directive. Taking into account the economic model of its business and the role comments play in it, it was decided that the company has control over user generated content.[165] After the final decision, Delfi decided to create a team of moderators to avoid liability for users' comments in the future. The company decided to also send an application to the ECtHR stating violation of article 10 of the Convention – the right to freedom of expression.

2.3.2. Chamber judgment

As far as the admissibility of the application was concerned, the ECtHR decided that even if the company was not an author of statements, holding the company liable as a publisher made it possible to benefit from protection of article 10.[166] Therefore, it was decided that the case would be examined on a merits basis. Both parties agreed that civil liability constitutes infringement of article 10; the discussion concerned what the role of Delfi was and what liability regime should be applied.

The applicant argued that its freedom of expression was violated without being prescribed by law. According to its argumentation, Estonian law prescribes only a negative obligation not to publish defamatory comments, but is silent about positive obligation to monitor allegedly

[165] Paras 27-29.
[166] Para 50.

defamatory content.[167] Moreover, Delfi claimed that the law was interpreted incorrectly (wrong understanding of the scope of legislative safe harbour in EU) and limitation was not necessary in a democratic society. There were other ways of protecting reputation prescribed by law than suing an ISP, such as sending a notice or civil litigation against the author of the comment.[168]

Estonia presented a different legal interpretation. Firstly, joint liability of the publisher and author of the publication is provided in case law and the Obligation Act; these were a basis for holding Delfi liable. As to the necessity in a democratic society, Estonia argued that reputation is a value that needs to be protected. Moreover, the Internet provides the possibility to disseminate vulgar and degrading comments very quickly, therefore it is up to the company to control the content and Delfi's actions were not effective. According to the Estonian government, Delfi cannot benefit from the safe harbour provision, since it is not a mere hosting provider, but has effective control over stored data (e.g. comments can be deleted only by Delfi).[169]

The Court based its reasoning on the argument that the ECtHR's role is not to replace national courts – therefore if in Estonia it was decided that Delfi falls outside of the scope of safe harbour provision, this is so.[170] The ECtHR was satisfied with the level of law foreseeability and commented that applying publisher regime to ISPs can be perceived as adapting legal measures to new technologies.[171] As to legitimacy of interference, the Court decided that "the fact that the actual authors were also in principle liable does not remove the legitimate aim of holding the applicant company liable for any damage to the reputation and rights of others".[172]

[167] The controversial legislation is the Obligations Act (Võlaõigusseadus) of 29 September 2001.
[168] Paras 52-58.
[169] Paras 59-67.
[170] Para 74.
[171] Para 75.
[172] Para 77.

Assessing "necessity in democratic society", the Court took into account four factors, namely: the context of the comments, the notice and take down procedure applied by the applicant, the liability of the authors of the comments and "the consequences of the domestic proceedings for the applicant company".[173]

The Court decided, that taking into account the controversial topic of the article, the company was aware of "a higher-than-average risk" of defamatory comments and should have taken proper measures to prevent or remove them. Notwithstanding a "word-based filter" necessity and a notice mechanism, they both failed in the described case. It was the company (not a person whose rights were infringed or an author of the comment) that was in the position of removing, blocking and preventing comments and it did not do any of these.[174] The court concluded also that the Estonian court did not oblige the company to use any specific form of prior monitoring, but left the broad scope of discretion as long as the aim is achieved – protection of the reputation of others.[175] Therefore there was no exceeding interference in the Delfi business model.

The ECtHR also did a balancing exercise, weighing protection of reputation provided by article 8 and anonymity of Internet users. In the Court's opinion, suing the author of the comment was not a sufficient measure to protect reputation due to the fact that the identity of users is generally very challenging to be established and often oversteps the possibilities of regular people who want to bring a claim.

To sum up the ECtHR's reasoning, there was no violation of article 10 (decision was taken unanimously), because "the comments were highly offensive; the portal failed to prevent

[173] Para 85.
[174] Para 89.
[175] Para 90.

them from becoming public, profited from their existence, but allowed their authors to remain anonymous; and, the fine imposed by the Estonian courts was not excessive."[176]

2.3.3. Comment

In my opinion, the decision of the Court has to be perceived as very regressive.[177] The Court, for the very first time, was given a perfect opportunity to evaluate the ISP liability in the context of defamatory anonymous comments and simply declined to do so. Moreover, it was a chance to elaborate on other issues related to ISP liability and notice and take down, such as procedural guarantees. The Court's approach can be perceived as very cautious, taking for granted that all notifications are made in good faith and Internet filters are a perfect solution for any kind of rights' infringements. The decision also shows a misunderstanding of issues such as how the Internet works and the stakeholders involved.

The greatest failure of the decision is, in my estimation, the lack of a human rights assessment of the safe harbour provision of the E-Commerce Directive, in the process treating the regulation as almost irrelevant. Without an understanding that ISPs are given legislative safe harbour, but also an obligation to take down content after notification, the proper assessment of the facts of *Delfi v Estonia* is impossible. The Court's decision makes article 14 of the Directive to be treated as insufficient and therefore creates legal uncertainty, creating different thresholds for ISPs under EU law and CoE obligations. Of course, it was not up to the ECtHR to

[176] Press release issued by the Registrar of the Court, ECHR 294 (2013), 10 October 2013.
[177] It is also a view shared by many freedom of expression and anti-censorship organizations, such as Article 19 in the statement of Guillemin, Gabrielle, "European Court strikes a serious blow to free speech online", 14 October 2013, available at: http://www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online, last accessed on 18 October 2013.

assess EU measures, but it could easily point out that Estonia interpreted the safe harbour mechanism wrongly and such an understanding has a negative effect on the free flow of information online.

Interestingly, the Court very easily reached the conclusion that it is the obligation of the ISP to prevent obviously illegal comments from being published. As in the case of pornography, the situation is pretty straightforward; I find it extremely difficult to assess with legal certainty which statement is defamatory, since the decision is based on various factors -not only the pure content of the statement or opinion. Therefore, I cannot imagine ISPs having knowledge, skills and resources to evaluate each comment with special care – we can predict that ISPs actions will now lean in the direction of taking down content without proper human rights evaluation.

I do not agree with the Court's approach that the matter of how high (or low in this case) the award of damages are should be taken into consideration. The question is if Delfi should be held civilly liable for the comments posted in this very specific case. The question is no, since the company deleted the comments immediately after receiving notification, as is provided in the E-Commerce directive. The ECtHR makes EU regulation simply insignificant and marginal, since they do not provide protection for ISPs.

The decision raised the serious and alarming question on the future of anonymous comments online. On the one hand, the Court emphasized the role of anonymity on the Internet, on the other it justifies civil liability by linking comments to the commercial benefits of Delfi. Moreover, the court did not give any specific hints and guidelines on how to protect reputation online; the measures to be implemented were left to the discretion of ISPs.[178] The easiest way

[178] "As regards the measures applied by the applicant company, the Court notes that, in addition to the disclaimer stating that the writers of the comments – and not the applicant company – were accountable for them, and that it was prohibited to post comments that were contrary to good practice or contained threats, insults, obscene expressions or vulgarities, the applicant company had two general mechanisms in operation. Firstly, it had an

can be to ban anonymous comments and introduce some mechanism of user verification and registration.[179] The introduction of such an approach will dramatically change the character of online comments threads and limit the Internet as an environment for free expression. Some claim[180] that it could even result in shutting down the comment option on webpages dealing with divisive issues.

Speaking for myself, I find the Court failing to implement its own standards which were described in previous parts of the chapter. Some can argue that the Court decided to implement a new approach with regard to the Internet case and since it was the first one of such character, the Court legitimately did so. The flaw of such an approach is the fact that the CoE has already developed basic standards of ISP liability in principle 6 of the Declaration on freedom of communication on the Internet.[181] In the *Delfi v. Estonia* case, the ECtHR decided to

---

automatic system of deletion of comments based on stems of certain vulgar words. Secondly, it had a notice-and-take-down system in place according to which anyone could notify it of an inappropriate comment by simply clicking on a button designated for that purpose, to bring it to the attention of the portal administrators. In addition, on some occasions the administrators of the portal removed inappropriate comments on their own initiative. Thus, the Court considers that the applicant company cannot be said to have wholly neglected its duty to avoid causing harm to third parties' reputations. Nevertheless, it would appear that the automatic word-based filter used by the applicant company was relatively easy to circumvent. Although it may have prevented some of the insults or threats, it failed to do so in respect of a number of others. Thus, while there is no reason to doubt its usefulness, the Court considers that the word-based filter as such was insufficient for preventing harm being caused to third persons." – the steps taken by the applicant were used against him and the Court did not elaborate on what proper steps should have been taken by the ISP to prevent civil liability – para 87.

[179]It is difficult to see how any site would allow anonymous comments if this ruling stands as precedent – Reidy, Padraig, "European ruling spells trouble for online comment", 11 October 2013, available at: http://www.indexoncensorship.org/2013/10/european-ruling-spells-trouble-online-comment/, last accessed 15 November 2013.

[180] Guillemin, Gabrielle, "European Court strikes a serious blow to free speech online", 14 October 2013, available at: http://www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online, last accessed on 18 October 2013.

[181]"Member states should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity.
Member states should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet.
In cases where the functions of service providers are wider and they store content emanating from other parties, member states may hold them co-responsible if they do not act expeditiously to remove or disable access to

implement a higher threshold of ISP liability than is provided in any international document on human rights.

What is interesting is that the evaluated case is an example of how the ECtHR refers to the jurisprudence of the CJEU.[182] The Strasburg court examines only the main points of judgments of the CJEU, without comparing factual and legal situations. Such an approach leads the ECtHR to misleading conclusions that previous decisions of the CJEU are in accordance with the Court's decision on limiting the nature of article 10. The decision is evidence for the lack of understanding of EU e-commerce's legal framework and its significance for freedom of expression. Sadly, the CJEU appears to be more protective towards the Internet and its role in enhancing freedom of expression than the ECtHR.

Delfi AS v. Estonia is not a final judgment and for sure will be referred to the Grand Chamber. The decision has to be perceived as an exception from previous court jurisprudence. It is not surprising that public opinion and freedom of expression activists were surprised by the decision.[183] The question is whether such an approach will become the norm or if the will Court will decide to apply its own standards more carefully, taking into account the specifics of the Internet. The decision can be interpreted as an attempt to protect individual freedom from large

information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.
When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information.
In all cases, the above-mentioned limitations of liability should not affect the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law."

[182] Paras 43-45 - the Court took closer look to decisions evaluated in chapter 2.
[183] More comments can be find in Nyman-Metcalf, Katrin "Legal Lens: What Delfi v. Estonia Says About Internet Freedom", 14 October 2013, available at: http://www.albanyassociates.com/notebook/2013/10/legal-lens-what-delfi-v-estonia-says-about-internet-freedom/, last accessed on 18 November 2013.

companies such as Delfi, but the same standards can be applied to a single blogger and this is a scenario that the ECtHR did not take into account.

Without a doubt, the notice and take down procedure should be evaluated from a human rights perspective. Of course, the EU is not party to the Convention (yet) but the CJEU reiterated that the Convention is part of the European legal order binding for the Community.[184] Moreover, the EU developed a mechanism to ensure that any legislation is human rights-proof. On the other hand, all members states of the EU, being at the same time parties to the ECHR, were obliged to implement the E-Commerce directive, as well as fulfil human rights obligations. Even dealing with seemingly commercial matters such as ISP legislative safe harbour, human rights have to be taken into consideration. Therefore challenging the directive might be problematic, but scrutiny towards implementing laws is rational.

Comparing substantial and procedural guarantees related to ISP liability and the ECtHR approach to the issue in *Delfi v Estonia* demonstrates how many questions still remain unanswered in the human rights area and that nothing can be taken for granted. Human rights, protection of freedom of expression and reputation are questions that must still be constantly addressed – right now in my opinion it is an appropriate time to deal with ISP liability and reconsider which approach should be chosen.

The chapter demonstrates that the issue of ISP secondary liability combines various issues such as freedom of speech, defamation claims, state limitation of free speech, procedural guarantees, choice of jurisdiction and many others. Therefore the issue of ISP liability from

[184] Arnull, Anthony, "The European Union and Its Court of Justice", Oxford: Oxford University Press, 2006, pp. 339-40.

a human rights angle in chapter 4 must be examined with certain concerns related to all these areas.

CHAPTER 3 – ISP SECONDARY LIABILITY – CASE STUDY: POLAND

EU member states, being members of the CoE at the same time, when dealing with ISP liability are obliged to take into consideration both community legal measures and human rights protection legal framework. Those two aspects of ISP liability were described in the previous chapters. Therefore, this chapter evaluates how a particular member state – Poland – deals with both the frameworks and the specifics of ISP liability at the national level.

Poland is an interesting example to scrutinize. Firstly, the implementation of the directive is not verbatim – in this case some more detailed legal constructions are introduced, but still a lot of question marks were left to the discretion of courts dealing with specific cases. Secondly, the ISP issue has been vividly discussed lately, mostly due to the efforts of civil society organizations.[185] The analysis shows that ISP liability is a very sensitive issue and we cannot conclude that there is legal certainty in this respect.

The chapter begins with addressing the issue of Polish legislation on ISP liability – this part shows how the E-commerce directive was implemented and, moreover, what are the strengths and the flaws of such regulation. Afterwards, a few cases are presented, all dealing with defamation online and ISP legislative safe harbour. Comparing those two rules with judicial practice makes it possible to assess the legal situation and to pinpoint the failures of Poland in creating a certain legal framework for ISP liability.

[185] Such as Panoptykon (www.panoptykon.org) and Helsinky Foundation for Human Rights (www.hfhr.pl).

3.1. Poland – ISP liability legal framework

Elaborating jurisprudence of any country is impossible without understanding the legal framework. The first part of this chapter introduces the Polish legislation concerning ISP liability. Poland transposed the E-Commerce directive into the national legal system by enacting Act of 18 July, 2002, on provisions of services by electronic means (hereinafter: the E-services Law).[186]

In Poland, there are two scenarios of holding ISP liable for user generated content in defamation cases. Firstly, there is criminal defamation described in the Article 212 of the Criminal Code.[187] Secondly, the articles 23-24 of the Civil Code regulate civil defamation based on personal rights (reputation) protection.[188]

3.1.1. The E-services law – ISP legislative safe harbour

The E-service law implements parts of provisions from the E-commerce directive into the Polish legal system. The scope of the legislation covers 3 broad areas: responsibilities of companies that provide e-services, liability exemptions for ISPs (legislative safe harbour) and the rules that protect the data of people who use e-services. As in the E-Commerce Directive, the E-services law regulates only the negative aspects of liability, namely exemptions from liability regime provided in other bills, such as the Civil and Criminal Codes.

Liability exemptions provided in chapter 3 of the E-services law can be applied only in cases of intermediary service providers – hosting providers are not covered by legislative safe

[186] Act of 18 July, 2002, on provisions of services by electronic means, official journal no.144, item 1204, as amended.
[187] Polish Criminal Code of 6 June 1997, official journal no.88 item 553, as amended
[188] Polish Civil Code of 18 May 1964, official journal no 16, item 93, as amended.

harbor.[189] The catalogue of entities benefiting from provisions is exactly the same as provided in the E-commerce directive. What is important, determination to which category ISP should be attributed is related every time to specific activity, not to the general business description of the company.[190] Liability exemptions are possible in all regimes: criminal, civil and administrative. The overall rule is that liability can be exempted in case of lack of factual knowledge about infringing content – more specific regulations provide different liability thresholds for conduit, catching and hosting providers.

Legislative safe harbour provision for host providers, implemented in article 14 of the E-services Law, is applicable when the ISP is not aware of illegal content and, after receiving either reliable or official notification, blocks access to the content. The provision is applicable to both civil and criminal cases – comparing to the directive which establishes two separate schemes.[191] Thus, the threshold for legislative safe harbour in civil cases is mitigated in comparison with EU level, which is an acceptable situation taking into account that the directive establishes maximum requirements of liability exceptions and these requirements can be lower in national legislations.[192]

The general rule forbidding posing an obligation of prior monitoring of the content by ISP is applicable to all types of safe harbour provisions .[193] Therefore, to hold any ISP liable,

[189] Litwiński, Paweł, „Świadczenie usług drogą elektroniczną" [E-services] in: Paweł Podrecki; „Prawo Internetu" [Internet law]; Warszawa 2007; p. 212.
[190] Okoń, Zbigniew, "Oskarżony: ISP – odpowiedzialność dostawcy usług internetowych" [Accussed: ISP – liability of e-services providers], IDG - International Data Group, 1 December 2000, available at: http://www.internetstandard.pl/artykuly/277675/Oskarzony.ISP.odpowiedzialnosc.dostawcy.uslug.internetowych.html, last accessed on 10 September 2013.
[191] Kuczerawy, Aleksandra; „Odpowiedzialność dostawcy usług internetowych" [ISP liability], available at: http://cbke.prawo.uni.wroc.pl/files/ebiuletyn/Odpowiedzialnosci_dostawcy_uslug_internetowych.pdf, last accessed on 10 September 2013, p.4.
[192] Podrecki, Paweł; „Prawo Internetu" [Internet law]; Warszawa 2004, p. 212.
[193] Article 15 of the E-services Law.

it is necessary to establish if the company really "knew" about the infringement, not only "should have known".

3.1.2. Act on provisions of services by electronic means – notice and take down

The Polish legislator decided to remain silent about any specific requirements or procedural steps concerning notice and take down procedure. Whereas "official notification"[194] is a notion easy to interpret, the legislator did not specify what "reliable notification" means – the prerequisites of initiating the procedure are only named, without explaining their exact meaning. It fails to address what makes notification "reliable", what data has to be given, what form of delivery it should have. Some people claim that any form of notification should be perceived as sufficient to waive the liability exceptions.[195] The more popular approach is that the notification to be treated as reliable has to be subjectively and objectively reliable.[196] Therefore, the notification should not only be reliable for the author, but moreover for the recipient, and some facts and proofs have to be included. Obviously, those are all postulates of doctrine, whereas the issue is not regulated by legislative measures.

The decision whether to block content or not in the case of receiving reliable notification was left to the discretion of ISPs. In practice, the decision is made by assessing eventual contractual liability. The legislator concludes the situation of preparatory papers to the E-services

[194] Understood as a decision of a court or an administrative body.
[195] Pacek, Grzegorz; „Jak należy uregulować odpowiedzialność za treść w Internecie? Wybrane aspekty" [How to regulate ISP liability for USG? Chosen aspects]; article prepared for NGO Panoptykon; available at: wolnyinternet.panoptykon.org/sites/default/files/pacek.pdf, last accessed on 13 October 2013, p.12.
[196] Pacek, Grzegorz; „Jak należy uregulować odpowiedzialność za treść w Internecie? Wybraneaspekty" [How to regulate ISP liability for USG? Chosen aspects]; article prepared for NGO Panoptykon; available at: wolnyinternet.panoptykon.org/sites/default/files/pacek.pdf, last accessed on 13 October 2013, p.13.

Act by stating that: "An ISP, being aware of the illegal nature of certain content, has to assess the legitimacy of notification".[197] This shows that in case of Poland the broad discretion of ISPs is not only an accidental result of implementation of the directive, but a conscious decision of the legislator. Moreover, any form of putting back the content is not provided in the legislation – therefore the Internet user is deprived of almost all guarantees to use his right to publicize content online.

Poland is the only country in the EU that protects ISPs from contractual civil liability[198] towards an author of blocked/removed content.[199] The protection is granted automatically only in the case of "official notification" - in the situation of receiving "reliable notification" the ISP is also obliged to inform the author of the content about the notification. There is no specification of neither the form in which ISP is required to contact the author, nor the promptness of ISP actions..

Theoretically, such a solution strengthens the protection of ISPs and creates a situation where ISPs should not be afraid of contractual liability. Surprisingly, taking into account the amount of cases related to ISP secondary liability (a few every year) and comparing this number to the number of e-services and its rapid growth, it can be concluded that the provisions are created in a way that discourages citizens from using them.[200] Understandably,

[197] Konarski, Xawery; „Komentarz do ustawy o świadczeniu usług drogą elektroniczną" [Act on provisions of services by electronic means – commentary], Warszawa, 2004, p.144.
[198] Usually users and ISPs are bind by terms of service of a specific ISP and taking down the content posted by the user can create contractual liability.
[199] Article 14(2)(3) of the E-services Law – in the case of "official notification" the exception is automatic, but after receiving the "reliable notification" the ISP is obliged to notify the author of the content before taking the content down.
[200] Wiewiórkowski, Wojciech; "Wyłączenie odpowiedzialności usługodawcy świadczącego usługę drogą elektroniczną za niektóre rodzaje usług" [Exeptions from ISP liability] , *Gdańskie Studia Prawnicze*, issue 21, 2009, p. 201.

the discussion on the law's amendment has been vivid in Poland for a few years – the issue is described in chapter 4.

The self- or co-regulation is not a very popular approach in Poland and there is no state regulation on notice and taking down at the level of any association of intermediaries.[201] Nevertheless, some companies decided to implement their own rules of conduct, e.g. Allegro developed "Cooperation for the Protection of Trademarks". [202]

As described above, Polish implementation is almost verbatim and so vague and brief as the directive. Without doubt, Polish authorities made some appreciated decisions while implementing the E-Commerce directive, however there are still many concerns requiring attention and discussion. Many significant questions related to ISP liability were left for court decisions and are decided on case-by-case bases, which is the subject of the next part of chapter 3.

3.2. Polish jurisprudence on ISP secondary liability

Even if Poland is an example of a country from civil law culture, not only legislative measures should be taken into account assessing how ISP liability regime works. . Especially in the area of social life where fast development can be observed (without doubt ICT is one of them), there is a significant role of courts and jurisprudence. Moreover, as shown above, the E-

[201] http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/poland_12nov2007_en.pdf, last accessed on 17 November 2013.
[202] "Polish E-Bay".

services act introducing legislative safe harbour leaves many question marks to be answered by courts. Therefore this part examines selected courts' decisions in cases concerning ISP liability.

Cases are presented in order according to the rendering date.. The analysis and conclusions are presented in the last part of the chapter. The presented selection is, according to my knowledge, the fullest attempt to present Polish jurisprudence on the issue of ISP liability so far.

3.2.1. Case A: Dariusz B. v naszaklasa.pl[203]

Naszaklasa.pl is the biggest Polish social networking service (comparable to Facebook), which enables its users to connect with each other, post comments, search for people you know – namely to perform various kinds of Internet interaction. Dariusz B. never used naszaklasa.pl, but his fake profile account, containing defamatory statements, was created by an unknown third party. Dariusz B. notified naszaklasa.pl about the alleged infringement by sending various e-mails and regular mails. None of them was received by the company due to misinformation about contact details on company's webpage. Even though the way of notifying the company was not in accordance with the terms of service, the company was held liable in civil proceedings for not removing the account promptly.

The Appellate Court concluded that naszaklasa.pl as a non-moderated platform can benefit from hosting ISP legislative safe harbour, but in this case it was excluded by company negligence. The company did not notify people about their actual e-mails and mail address. Therefore, even if the company was not aware of the infringement, it should have been aware

[203] Appellate Court in Wrocław, 15 January 2010, I ACa 1202/09, published in OSAW 2010/2/167.

since the notifications were sent via various channels consistent with information on the company's webpage. The case was a chance to elaborate on the form of notice which can be treated as triggering ISP liability. The Court held that the specific form required by the company in terms of service can be applicable only to portal users and any other person can notify the company in any form. Therefore such a notification is not bound by any specific requirements as to what it should consist of – therefore e-mails sent by Dariusz B. were treated as sufficient to initiate the obligation of ISP to take down content.

Not only did the court take a stand in legal questions crucial for the case, but it also elaborated more on the nature of legislative safe harbour. The Court found it unacceptable to require hosting ISPs to monitor and filter content which can happen to be infringing as it violates both 14 and 15 article of the E-services Law. The plaintiff claimed that due to the professional nature of the company, the activity standards of prior monitoring should be higher than for random Internet users, such as bloggers. The view was not shared by the Court at the appellate level. Worryingly, this argument was accepted by the court of first instance.[204]

The terms of service of naszaklasa.pl consists of provisions stating that in case of any notification the company has 14 days to take a stand, evaluate the legal situation and take appropriate steps (refusing introversion, block or take down content). Nevertheless, the court stated that 14 days is too long a period to assess defamatory charges and the company should, for the time of assessing legal character of notification, at least block access to the content. The Court did not use the opportunity to include the author of the content into the notice and take down procedure, nor create the proper conditions and legal framework to enable ISPs to take decisions not automatically or without due diligence.

[204] I C 625/08, District Court of Wrocław, 31 July 2009, not published yet.

The decision was perceived as a precedent for various reasons. Firstly, it was stated that civil liability in defamatory cases can be based on omission, not only on actions as it is usually perceived in the Polish legal doctrine. Moreover, it was clearly stated that legislative safe harbour can be applied also to cases of infringement of personal interests, which was not clarified so far (provisions of the E-services Law were simply omitted in the decision process of personal interests online). Lastly, the court appeared to be pretty progressive (even with my disapproval of its approach to the issue of time for the company decision process), deciding also on issues not necessary related to the case, but to the broader concept of ISP secondary liability. What is important is that it was underlined that every hosting ISP is obliged to create an effective and simple system of notifying an infringement.

3.2.2. Case B: Balus v mayor of Kalwaria Zebrzydowska[205]

This case refers to the very important question of how to set the line between scope of application of the Press Law and the E-services Law. The Polish Press Law comprises a very broad definition of the press, provided in article 7 para 2. The definition includes also "any means of mass media, existing or appearing as a result of technical progress, including (…) all systems that broadcast publication periodically as print, picture, sound". Therefore ISP liability cases sometimes happened to be considered under this provision. Traditionally, the state regulates the press in more detailed than the Internet – and such an approach results in stricter ISP liability regime.

The mayor of Kalwaria Zebrzydowska felt offended by comments posted on a blog owned by Mr. Balus and decided to bring a suit in civil proceedings to protect his reputation.

[205] Krakow Regional Court, I C 1532/09, of 11 March 2010, not published yet.

Comments were made by an anonymous user and the blogger refused to delete them due to the fact that these were opinions of inhabitants of Kalwaria Zebrzydowska and they had the right to exercise their freedom of expression. Moreover, the defendant raised the issue that in his opinion those statements did not have a defamatory character.

The court dismissed a civil complaint by the politician against the blogger. The Court found that an internet portal does not fall within the definition of press. Therefore the threshold of professionalism and legal risk are lower for ISPs than for printed, traditional media.

The court used the case also to elaborate on the difference between the languages used in printed media and online. The Internet, as an environment open to various actors, is characterized by different language, more shocking and controversial – therefore high standards of what is defamatory and what is not in the press (only so called "literally language" is acceptable) cannot be directly imposed on ISPs. Moreover, the language of public debate is usually more vivid and politicians should be aware of being exposed to public scrutiny.

There is also an assessment of risk of censorship privatization in the court's judgment. It is said that a single person, such as a blog owner or a forum moderator is not able to control all user-generated content. Imposing such an obligation will facilitate a change in the mode of Internet functioning by only big ISPs being able to operate without extended risk of potential liability. Without proper application of ISP legislative safe harbour by courts, ISPs will find themselves in the position of judges, being forced to assess which content is infringing and which is lawful. ISPs lack not only knowledge and skills to assess such issues, but above all competence – it is up to the judiciary to decide what is legal and what is not.

3.2.3. Case C: Jezior v mayor of Ryglice[206]

The judgment was rendered in election procedures (which shows also how ISP liability issue can be used as a political tool). Some comments about the mayor of Ryglice were published on a blog run by Jezior. The comments were deleted by the blogger on his own initiative or just after receiving notice from the mayor every time. Nonetheless, the mayor decided to initiate trial in the election procedure to get protection for his reputation.

The blogger was held liable and forced to publish apologies in the local newspaper and to donate a certain amount for charity purposes. The court found the excuse that users were using their freedom of expression insupportable and therefore the blogger cannot be held liable for somebody else's words. Moreover, the Court reasoning was based on the statement that having a blog and enabling posting of anonymous comments should be treated as wrongdoing, which is a prerequisite for suing somebody for defamation. The blogger was the one in the position of ensuring that only true statements are published via e.g. introducing a logging obligation, but he did not decide to do so – the fault of the blogger is based on omission.

According to the court, any blogger can be held liable for the comments of users due to the fact that they are not only liable for the content of the articles, but also for the mere fact of introducing the option of commenting. Such an approach is based on the reasoning that a blog combines both articles created by bloggers and user-generated content – deciding on such a business model is linked to risk of liability.

The blog was political and addressed the issues that were controversial for the local community The Court held that the blogger, being aware of the political and sensitive nature of a possible discussion on the blog, should have created a functional system of avoiding

[206] District Court in Tarnów, 15 November 2010, I Ns 162/10, not published yet.

defamatory comments. Especially such a mechanism is needed in times of election, when comments can hurt politicians.

The Court does not refer at all to ISP secondary liability and legislative safe harbour provided in the E-services law. The case is an example of deep misunderstanding of who should be treated as ISP and which law should be applied in defamatory cases online (the court relied only on the civil code). Moreover, some alarming approaches were reflected, e.g. imposing stricter threshold of liability for bloggers involved in political activity.

3.2.4. Case D: Akademicka Oficyna Wydawnicza case[207]

Akademicka Oficyna Wydawnicza is a publisher of a regular magazine "Forum Akademickie" which also has an internet version. It is possible to comment on articles online. The company was sued for defamatory comments posted under a text about the rector of one university. The Court of first instance[208] dismissed the case, stating that the comments were deleted promptly after notification, therefore the unlawfulness of the company act was excluded and made it impossible to be held liable for comments by a third party. The court did not find reasons to evaluate the case from press law perspective.

The case was re-examined by the Appellate Court which came to completely different conclusions. The question was raised of when the company got to know about infringing content. The court of first instance came to the conclusion that the notification is an obligatory prerequisite of waiving legislative safe harbour. On the contrary, the appellate court noticed that the company hired a moderator and also posted an on forum warning, that comments

[207] Appellate Court in Lublin, 18 January 2011, I Aca 544/10, published in LEX no 736495.
[208] District Court in Lublin, 25 June 2010, I C 618/09, not published yet.

can be moderated. Therefore, it has to be assumed that the company became aware of infringing content before notification (which was sent a few months after the comment was published) and, hence it was held civilly liable.

The court decide to add an additional factor to evaluation of ISP liability, namely the presence or lack of a moderator and factual possibility of becoming informed about the infringing content (not factual knowledge, but only possibility).

3.2.5. Case E: judgment of the Supreme Court of 8 July 2011[209]

This case refers to civil liability for defamatory statements directed towards the author of the article about engagement of a politician in a sexual affair. The politician was a mayor of a town. An unknown user, using an IP publicly available Wi-Fi network, posted defamatory comments questioning the intentions of the author. The author sued the town's authority for infringements of personal interests – comments were published on the webpage hosted by the town.

The Supreme Court decided that any form of providing a platform to exchange comments is generally within the scope of legislative safe harbour. Therefore there are only two scenarios in which hosting ISP can be held liable for infringements of personal interests: if the company knows about the infringing character of the content or if it does not delete the comment after receiving reliable notification. Moreover, this is not up to the ISP to reveal the identity of the user to enable civil case – this factor cannot be taken into account while assessing ISP secondary liability. None of the provisions of the E-services Law creates the legal obligation to

[209] The Supreme Court of Poland judgment, IV CSK 665/10, published in OSNC 2012/2/27 and M. Prawn. 2012/10/537-540.

reveal the identity of a user as a pre-requisite of legislative safe harbour and, therefore, such an approach is unacceptable. Therefore the case was dismissed

The decisions taken by the Supreme Court (which means that other courts should rely on its reasoning and legal interpretation) should be perceived as creating a very broad catalogue of companies secured by legislative safe harbour. Moreover, the onus of establishing who is the author of infringing content was taken away from ISPs and shifted towards the person whose right was violated – before the question was disputed.

3.2.6. Case F: Jezior v mayor of Ryglice – part II[210]

The first part of *Jezior v mayor of Ryglice* was decided in a special judicial procedure – election, which enables securing rights of politics during a political campaign. The mayor decided also to sue the blogger in regular civil proceedings for defamatory comments published by a third party.

In civil proceedings the court of first instance[211] took into consideration the fact that Jezior is also a person involved in local politics and, as such, he should have been aware that blog activity can result in heated debate. Defamatory comments and false statements are an inseparable part of such a debate. Therefore, he should create some system of monitoring comments (blog platform he was using had various options, including blocking comments option or prior moderation). The district court determined also that the lack of action for defamatory comments, even without any form of notification, results in waiving legislative safe harbour. Therefore the blogger was held liable.

[210] Appelate Court in Kraków, 19 January 2012, I ACa 1273/11, not published yet.
[211] District Court in Tarnów, 3 October 2011, I C 319/11, not published yet.

The Appellate Court quashed the decision of first instance and was more favourable towards the blogger. Firstly, the court underlined that in order to be held liable for infringement of personal rights, the action or the omission being the base of the liability has to be unlawful. Therefore any defamatory comment online should be evaluated using a two-step test. Firstly, the scope of civil code has to be assessed in the context of personal rights. Afterwards, it has to be evaluated if the situation falls within the scope of legislative safe harbour, since article 14 of the E-services Law precludes unlawfulness of action or omission. It does not mean that article 14 excludes provisions of the civil code, but only unlawfulness (which was misunderstood by the court of first district).

Moreover, it was directly stated that there is no reason to evaluate ISP liability through the perspective of the mechanism used on the blog enabling posting comments. There is no legal obligation to require registration of users and therefore the lack of such procedure cannot be interpreted against the blogger. There is no possibility of linking the ISP liability to the issue how possible it is to find out who was the real infringer.

The Court underlined that the scope of ISP liability regime is related to the nature of the Internet and its aims, namely enabling users to exercise the right of freedom of expression without state intervention – therefore any limitation of ISP liability has to assess from a human rights perspective as well. Consequently, any form of prior monitoring should be perceived as violation of freedom of expression. The Court as a result of the balancing exercise concluded that protection of other values (such as reputation) should not outweigh freedom of expression online.

3.3. Conclusions

After elaborating on both legislation and the courts' practices related to ISP liability it is possible to make some more general comments on this issue in Poland. The general conclusion is that poor and unspecific legal framework results in various, sometimes even opposite judiciary decision and such a situation do not secure freedom of expression and Internet users' rights.

3.3.1. Assessment of legal situation in Poland concerning ISP liability – general remarks

In Poland courts are not bind by the decision of other judges (as long it is not appellate decision in the same case or the decision of the Supreme Court). Polish examples show how inconsistent judicial approaches to the legislation related to ISP liability can exist. The reasons behind such a situation is poor, not specific and clear legislation. Leaving many legislative gaps, unanswered questions and no clear guidelines, results in a situation when very similar cases can be assessed very differently. What is interesting, is that the uncertain legal situation of ISPs becomes even more complicated after the courts' decision, not quite contrary as we would probably expect.

Firstly, it is worth examining the catalogue of cases presented above. Generally, there are only a few cases each year concerning ISP liability – therefore the catalogue is minimalistic – simply there is no more research substance. Of course, there are also cases related to other situations when ISP liability is an issue, such as IP protection, hate speech or pornography. Moreover, there is only one scheme that is repetitive, specifically that the person whose reputation was infringed sues an ISP. I did not encounter in my research any case of an author of the content suing an ISP for removing their content as a freedom of expression infringement.

Additionally, it should be taken into consideration who is usually the plaintiff in the evaluated proceedings – in almost all cases these are people involved in public activity (such as politicians). This does not imply that regular citizens' rights are not infringed online, but more probably shows that ISP liability can be used as a tool to limit public debate and that regulations concerning ISP liability are not so citizen-friendly to be used without appropriate awareness and resources.

The narrative of these decisions is also interesting. The courts usually refer only to the business and economic aspects of ISP liability, evaluating only the scope and of the E-services law (referring also to EU measures, as was in the case E). Only in case F the court elaborated on the human rights nature of ISP liability and how freedom of expression should be taken into consideration. But this part of the court's assessment was only additional and still it was not the main reasoning the judgment was built on. Even in interesting case B, while elaborating the risk of privatization of censorship, the court did not link the issue to the human rights narrative.

3.3.2. Assessment of legal situation in Poland concerning ISP liability – notice and take down

There are some cases when ISP safe harbour is not even taken into consideration, even if the case clearly addressed the issue of liability for user generated content (such as case C). Nevertheless, the catalogue of entities benefiting from legislative safe harbour is fairly well established (which is confirmed by the judgment of the Supreme Court). Also there is not much discussion on the issue in which situation ISP legislative safe harbour can be taken as an option (it was confirmed that it is surely the case with persona rights infringements in case A).

Worryingly, the factor that matters is that the scope of legislative safe harbour is slightly different in all evaluated cases and courts easily add additional requirements that have to be

fulfilled in order to benefit from liability exemption. These can be: obligation of prior monitoring due to the professional and commercial nature of the ISPs' activity (case A, first instance); higher threshold of liability in the case of having a moderator on the forum (case E); higher threshold of liability in the case of political bloggers (case C). Such a discrepancy results in contradictory decisions being taken in very similar cases, as in cases B and D – in both ISPs took content down immediately after receiving notification, but in the second case the court decided that ISP should have known and taken action even before notification.

The Polish judiciary system seems to be afraid of taking a stand on notice and take down procedure issue. In case A, the court had to consider very detailed terms of service, consisting of also regulated notice and take down procedure. Naszaklasa.pl's terms of service secured 14 days to make a decision after receiving a notice due to the company's own standard of notifying the author of the content about the complaint. 14 days give the opportunity to examine also the arguments of the other party of the dispute. The court shortly concluded that 2 weeks' time is too long and the ISP has to block access to content while making its final decision and therefore naszaklasa.pl was held liable. The issue of the role of the author of the content in the whole procedure was not mentioned. Moreover, question marks left by the legislator, such as which notification can be perceived as reliable or how to approach self-regulation of ISPs have not been even noticed by the courts.

It is no surprise that ISPs in Poland usually willingly block content just after notification, to exclude themselves from liability and not to take efforts in assessing the case. Data on this phenomena is not available, my general conclusion is based on the evaluated cases (the way ISPs acted in them) and my activity as a regular Internet user. To sum up, the trend shown in the Polish example is characterized by discrepancy of courts' ruling on ISP secondary liability due to

the vague legislation, neglecting human rights aspects of the issue and not answering on the judicial level the question left by the implementation of the E-commerce directive.

The chapter addresses the issue of national implementation (in Poland) of ISP legislative safe harbour on both legislative and judicial levels. The presented examples simply demonstrate that ISP liability legislation is not specific and legally certain enough to create a system where human rights are sufficiently secured. Private entities were given a great responsibility for dealing with content online and private censorship takes place only with regards to business and economic interests. By creating such legislative frameworks and constructions, Poland as EU member state gave priority to community obligation, neglecting its responsibilities as members of the CoE. The clash between human rights obligations and current rules and practice concerning ISP liability is summed up in chapter 4.

CHAPTER 4 – ISP LIABILITY – HUMAN RIGHTS CONCERNS

Addressing the Internet's ambiguous power to foster freedom of expression as well as to create new avenues of abusing this freedom requires carefully balanced legislation. Anonymity is certainly/undoubtedly a factor enhancing freedom of expression, especially in the most "sensitive cases" (when revealing identity might result in certain social sanctions, harassment or even legal prosecution).[212] On the contrary, however, this is also a challenge from an accountability perspective when the Internet is an arena of law violations - both in the case of criminal (pornography, slavery, money laundering) and civil (defamation, IP rights) liability.[213] Establishing who is responsible for certain unlawful conduct is sometimes impossible – it creates the threat that some victims will not get remedy because the identity of the infringer is inaccessible. It also undermines one of the aims of criminal law in general (its punitive function) and might result in lower public faith in law enforcement mechanisms and efficiency.

To avoid such a situation, the ISP secondary liability regime was introduced in the EU. There is a global consensus that ISPs should not be held absolutely liable for any user's illegal content.[214] Without a doubt, altered consensus will have a "chilling effect" on ISPs' commercial activities which are indispensable for the functioning of the Internet.

[212] Akdeniz, Yamanand and Horton Rogers, "Defamation on the Internet" in: Yaman Akdeniz, Clive Walker, and David Wall (eds.) "The Internet, Law and Society", Pearson Education Ltd., 2000, p. 294.
[213] Maclay, Collin, "Protecting Privacy and Expression Online" in Ronald Deibert and Initiative OpenNet (eds.), "Access Controlled : The Shaping of Power, Rights, and Rule in Cyberspace", Cambridge, MIT Press, 2010, p.99.
[214] Sutter, Gavin, "Internet Service Providers Liability" in: Mathias Klang and Andrew Murray(eds.) "Human Rights in the Digital Age", London GlassHouse, 2005, p.71.

The fact that both EU and national legislations leave ample room for ISPs' discretion about the form of the procedure and when such a procedure should be launched has led large companies to establish their own notice and take down procedure. As examples, Google[215] and Facebook[216] regulations can be mentioned. They prescribe what information should be given by users as well as internal corporate procedure for deciding on effectiveness and reliability of a notification. Neither of them provide any form of notification of users whose content was deleted or procedure of 'put back' in the case where the author proves that the content is not illegal. Such a situation raises various questions from a human rights perspective.

The chapter, condensing the knowledge and observation from previous parts of the thesis, addresses four issues crucial for the human rights evaluation of the ISP liability. Firstly, the risk of privatization of censorship online is assessed. Secondly, the question of procedural guarantees (or to be more accurate, lack of such) is evaluated. Here, some supplementary, not immediately evident, but relevant human rights concerns are raised. Finally, the possible scenarios of how to approach ISP liability and ongoing debates in the EU and Poland are described. All those considerations and remarks lead to the conclusion that in the current legal situation both the EU and member states have failed to regulate ISP liability in compliance with human rights standards.

[215] Removing content from Google, available at: http://support.google.com/bin/static.py?hl=pl&ts=1114905&page=ts.cs , last accessed on 7 November 2013.
[216] Facebook Statement of Rights and Responsibilities, available at: https://www.facebook.com/legal/terms, last accessed on http://support.google.com/bin/static.py?hl=pl&ts=1114905&page=ts.cs , last accessed on 7 November 2013.

4.1. The question of self-regulation on the Internet – risk of privatization of censorship

From a technical point of view, it is unmanageable/unfeasible to make the Internet totally censorable.[217]Any form and actions undertaken by governments can be subverted by hackers and IT specialists. Technical censorship online is the utopia. The question and concern remains how Internet actors use self-regulations. Such regulations might result in factual censorship of the content due to the threat of civil or criminal liability in such cases as pornography, hate speech or copyrights. This part particularizes the self-regulatory characterization of ISP secondary liability and its chilling effect.

4.1.1. Self-regulation online

The E-commerce Directive enhances the self-regulatory[218] approach to the ISP liability and notice and take down procedure: "drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organizations, designed to contribute to the proper implementation of Articles 5 to 15".[219]Self-regulation is understood in the EU as an example of an alternative method of regulation (contrary to the traditional legislation) being very useful in the situation of new technologies, very detailed and technical legal questions, or those in which many stakeholders are involved. It must also be borne in mind that

[217] Foley, Conor, "Human Rights and the Internet" in: "Liberating Cyberspace : Civil Liberties, Human Rights, and the Internet" edited by Liberty, Pluto Press, 1999, p.271.
[218] Understood as "the possibility for economic operators, the social partners, non-governmental associations or associations to adopt amongst themselves and for themselves common guidelines", European Union Inter-institutional Agreement on Better Lawmaking, 31 December 2001, Official journal C 321/01, para 22.

[219] Article 16.1(a) of the E-Commerce Directive.

EU legislation is subsidiary,[220] therefore self-regulation is a preferable approach to creating a legal framework. EU legislation should be an ultimate solution.

There are various types of self-regulation, ranging from post-publications (as notice and take action mechanisms, journalistic ethic bodies or any other system of monitoring, reporting and complaints) to systems of classifications, flirting or pre-rating.[221] All these measures results indirectly in a situation in which ISPs establish the scope of their legal obligation on their own due to the fact that the state left a legal gap or margin of appreciation for the measures used to achieve certain aims. Sometimes self-regulation might result in a higher degree of fundamental rights protection, although most often the scenario is reversed.[222]

Of course, self-regulation, especially in media, is perceived by many as much more effective tool and less restrictive measure than the one provided by states.[223] On the other hand, the issue becomes highly debatable when states hand over to private entities the regulation on fundamental rights.[224] The mechanism shifts public functions from authorities to private entities.

Various authors[225]have emphasized that the censorship phenomena online has shifted from states to private actors such as users, readers, ISPs. Users, operating in real societies, are bound by some social and moral norms that they try to impose online by the choice of content to which they want to have access– such practice results in individual self-regulation, not infringing access to the information of others. On the other hand, actions related to content taken

[220] The principle of subsidiarity is defined in Article 5 of the Treaty on European Union, Official Journal C 115/13.
[221]Tambini, Damian, Danilo Leonardi and Christopher T. Marsden, "Codifying Cyberspace : Communications Self-Regulation in the Age of Internet Convergence", New York : Routledge, 2008, 2008, p. 274.
[222] Garfield, Alan E., "Promises of Silence: Contract Law and Freedom of Speech", *Cornell Law Review*, Vol. 83, 1998, pp. 343-360.
[223]Tambini, Damian, Danilo Leonardi and Christopher T. Marsden, "Codifying Cyberspace : Communications Self-Regulation in the Age of Internet Convergence", New York: Routledge, 2008, 2008, p.269.
[224] Starr, Sandy, "Putting freedom back on the agenda: why regulations must be opposed at all costs" in: Christiane Hardy and Christian Möller (eds.) "OSCE Spreading the Word on the Internet - 16 Answers to 4 Questions", available at: http://www.osce.org/fom/13871, last accessed on 7 November 2013.
[225] As Newey, Adam, "Freedom of expression: censorship in private hands" in "Liberating Cyberspace : Civil Liberties, Human Rights, and the Internet", edited by Liberty, Pluto Press, 1999, p.15.

by ISPs somehow influence the Internet for all users and might be perceived as mass self-regulation. Of course, the first type is acceptable and more favourable than the second, which makes ISPs' powers dangerously similar to states'.

4.1.2. Negative aspects of freedom of expression

Self-regulation is one of the aspects of a broader debate on negative and positive rights online.[226] The first one assumes "freedom from" any forms of control or surveillance, the second "freedom to" open Internet, debates and public fora. The Internet is a very sensible environment for any form all individuals freedoms restrictions– one form of content regulation might create a "slippery slope" effect.[227] Any exemption from the rule "the best Internet policy is no Internet policy" threaten the marketplace for idea concepts and undermines public agreement on the Internet as an arena of free speech.

ISP secondary liability results in factual censorship which influences not only freedom of expression but also standards of reputation protection. Every time stricter liability regimes are imposed on IPSs, ISPs are forced to take on a role of regulatory agents. Users are thereby deterred from extending the scope of freedom of expression due to the fear of being cut off by ISPs.[228] This demonstrates that not enough safeguards were established to protect fundamental rights.

[226] Tambini, Damian, Danilo Leonardi and Christopher T. Marsden, "Codifying Cyberspace : Communications Self-Regulation in the Age of Internet Convergence", New York: Routledge, 2008, 2008, p. 285.
[227] Hosein, Gus, "Open Society and the Internet: Future prospects and Aspirations" in Christian Möller and Arnaud Amouroux (eds.) "The Media Freedom Internet Cookbook", Organization for Security and Co-operation in Europe, 2004, p. 250.
[228] Newey, Adam, "Freedom of expression: censorship in private hands" in "Liberating Cyberspace : Civil Liberties, Human Rights, and the Internet", edited by Liberty, Pluto Press, 1999, p. 34.

It is necessary to emphasize that the notice and take down procedure is not a matter of two players only (an ISP and the person who claims defamatory character of the statement), but the legal situation of the author of certain content is also influenced. But in practice usually the latter group has few, or even no possibilities of challenging the procedure.[229] It equates to a situation where the private entity has influence on fundamental rights, but the person whose rights are infringed upon has no possibility to go to a court – the ISPs are not obliged to protect and respect human rights and the whole procedure is according to the law.

Moreover, depending on the jurisdiction, ISPs are threatened not only by civil liability, but sometimes by criminal or financial sanction.[230] That results in ISPs taking too rapid a decision about the procedure – commercially oriented entities are the most concerned about the financial profits and are not obliged to provide transparent decision making process. Additionally, the notion of defamation is extremely broad and challenging even for judiciary bodies – ISPs are not necessarily the most suitable entities to decide on the nature on the content, not only due to the lack of human rights consideration, but simply lack of legal knowledge.

4.2. Assessment of ISP liability compliance with procedural guarantees

Notice and take down procedure is sometimes mistakenly perceived as a relation between only private actors – ISPs and individual users. According to the traditional approach to human rights enshrined in European constitutional law and human rights treaties, human rights apply

[229] Villeneuve, Nart, "Evasion Tactics: Global Online Censorship is Growing, but so are the Means to challenge it and Protect Privacy", *Index on Censorship,* Vol. 36 No. 4, November 2007, p.73.
[230] La Rue, Frank "The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 16 May 2011, A/HRC/17/27, available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf, last accessed on 7 November 2013.

vertically to public authorities vis-à-vis the individual.[231] With such an assumption, human rights cannot be invoked directly in the relationship between ISPs and their users because it is a purely private sector relationship. However, ECtHR referred in a few cases regarding Article 10 to the German concept of *Drittwirkung* – the horizontal application of human rights.[232] As was stated in *Fuentos Bobo v. Spain*,[233] the state is obliged to protect freedom of expression from threats by individuals and companies. The same approach was confirmed in the more recent *Palomo Sanchez and Others v. Spain*.[234] In the case a trade union activist was dismissed by a private company after a critical publication in a newsletter. Even if the court has not found the violation (the disciplinary measure of dismissal was found not disproportionate), it has underlined that the state is responsible for "a failure on its part to secure the applicants the enjoyment of the rights enshrined in Article 10 of the Convention". Such an approach was confirmed in the Resolution on the Protection of Freedom of Expression and Information on the Internet and Online Media[235] and Declaration of the Committee of Ministers of 29 September 2010 on network neutrality.[236]

[231] Garlicki, Lech, "Relations between Private Actors and the European Convention on Human Rights inThe Constitution" in András Sajó and Renáta Uitz (eds.) "Private Relations: Expanding Constitutionalism", Utrecht: Eleven International Publishing, 2005, p.129.

[232]Harris, O'Boyle & Warbrick, "Law of the European Convention on Human Right", Oxford University Press, 2009, pp.446-447.

[233] European Court of Human Rights, *Fuentos Bobo v. Spain*, application no. 39293/98, judgment of 29 February 2000, para 38.

[234] European Court of Human Rights, *Palomo Sanchez and Others v. Spain*, Application no. 28955/06, 28957/06, 28959/06, 28964/06 , judgment of 12 September 2011, para 60.

[235] "The Assembly calls on the member States of the Council of Europe to: ensure, in accordance with Article 10 of the Convention and the case law of the European Court of Human Rights, respect for freedom of expression and information on the Internet and online media by public as well as private entities, while respecting the protection of privacy and personal data" - Resolution of the Parliamentary Assembly of the Council of Europe, no. 1877 (2012) on The protection of freedom of expression and information on the Internet and online media, available at: http://assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=18323&Language=en, last accessed on 7 November 2013.

[236] "As regards procedural safeguards, there should be adequate avenues, respectful of rule of law requirements, to challenge network management decisions and, where appropriate, there should be adequate avenues to seek redress" - Declaration of the Committee of Ministers on network neutrality, adopted by the Committee of Ministers on 29 September 2010at the 1094th meeting of the Ministers' Deputies, available at: https://wcd.coe.int/ViewDoc.jsp?id=1678287, last accessed on 7 November 2013.

4.2.1. The role of procedural guarantees in notice and take down procedure

The problematic nature of notice and take down procedure is easier to be understood by evaluating an imaginary, but possible, factual case. X puts a comment under the article at issue being vividly discussed claiming that Y should be responsible for some misconduct. Y notifies the ISP (e.g. owner of the blog, as in the case of Google and its platform Blogger) that the comment is defamatory. The ISP, without great consideration, blocks the comment and… does nothing more.

The first scenario is that X never realizes that his comment was taken down – the ISPs are not obliged to notify individuals nor to announce the initiation of the procedure.[237]Without doubt, X'sfreedom of expression was infringed by the private actor. He cannot challenge the ISP's conduct in any proceedings due to this lack of awareness of a violation.

The second scenario assumes that X notices that the content was taken down – but of course was not provided with the reasoning behind this decision. He is deprived of the right to prepare civil proceedings – he does not know why his fundamental rights were infringed.

Due to the fact that the notice and take down procedure was established as a legislative safe harbour pre-requirement for ISPs by EU member states it can be claimed that states have a legal obligation to create legal frameworks respecting a "duty to give reasons". Such a right, to obtain/receive information why the content was taken down, can be secured of course also by ISPs in their self-regulatory mechanisms, but over all has to be guaranteed by member states which can impose an obligation for ISPs to respect "duty to give reasons". Both legal analysis and practise show it was not a case while implementing the E-Commerce Directive.

[237] Lack of such obligation in previously analyzed legislations and standard provisions in the E-Commerce directive.

4.2.2. Rule of law considerations

Looking at notice and take down procedure from a broader, rule of law context forces us to question the system as depriving the Internet user of any rights and guarantees. ISPs take decisions only on the basis of the notification and the user cannot present his opinion on the issue, which will result in infringing his fundamental right. Of course the presumption of innocence and right to defence are notions deriving from criminal procedure, but it seems preferable to create the space for adversial debate before deciding that the content is illegal. Moreover, the decision-making competence is shifted from judiciary body to private entity.[238]This is an ISP deciding if the statement should be perceived as defamatory or the content as breaching copyright. Of course its decision does not result in civil liability but in influencing the user's freedom of speech online.

Moreover, EU and Polish legislations seem to be disproportionate when the rights and guarantees of parties are evaluated. The conduct of the person notifying and ISPs are prescribed, but any obligations or rights of users whose content is taken down are not mentioned. Obviously, he can always try to bring civil complaint, but the comparison of efforts and money-consumption of both judicial proceedings and notice and take down procedure proves that the right to get his freedom of speech acknowledged and protected is more burdensome compared to how easy it is to block or delete content online.

[238] Tambini, Damian, Danilo Leonardi, and Christopher T. Marsden, "Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence", New York: Routledge, 2008, p.271.

4.2.3. Legal certainty concerns

Concerning both EU and national legislations leads also to legal certainty critique. Many notions are undefined, such as "credible notification" or "expeditious time" when ISPs are obliged to act. This results in ISPs' decisions to block access to infringing materials without any hesitation or consideration of the legality or illegality of the content.[239]Ultimately, the notice and take down scheme is incompatible with guarantee rights developed by the ECtHR and, moreover, withdraws judicial protection of freedom of expression, introducing private censorship dependent on private entities' reasoning and law interpretation.

4.2.4. General assessment of notice and take down procedure from procedural guarantees perspective

The development of the Internet frequently leads to novel legal challenges[240] – but the case of regulating ISP liability does not call for implementation of any new solutions, simply for the member states' application of the standards already established by ECtHR. The European Data Protection Supervisor is aware that low standards of guarantee rights equals a threat to substantive rights.[241] He calls for harmonization of the notice and take down procedure on the

[239] Sutter, Gavin "Internet Service Providers Liability", in: Mathias Klang and Andrew Murray (eds.) "Human Rights in the Digital Age". Edited by Mathias Klang and Andrew Murray, London : GlassHouse, 2005. p.77.
[240] Sutter, Gavin "Internet Service Providers Liability", in: Mathias Klang and Andrew Murray (eds.) "Human Rights in the Digital Age". Edited by Mathias Klang and Andrew Murray, London : GlassHouse, 2005. p.83
[241] EDPS formal comments on DG MARKT's public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, Brussels, 13 September 2012 available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-09-13_Comments_DG_MARKT_EN.pdf, last accessed on 7 November 2013.

community level – in other cases the level of protection will differ in various countries, which can result in problems taking into account the global character of the Internet.

The notice and take down procedure is not the only example of a situation where countries are unable to secure freedom of expression online according to the ECtHR standards. Another example worth mentioning are IP rights, access to information or states' attempts to combat unlawful activities on the Internet. All these situations are alarming from a procedural perspective – the prerogatives of private actors expand, while diminishing the role of the judiciary in protecting fundamental rights.

The described problem also illustrates a broader trend in the approach to human rights protection in the CoE. The world nowadays is progressing and developing so fast that it is impossible to create new standards applicable only for a certain situation. In my opinion the ECtHR jurisdiction is already well developed and therefore it is the states' obligation at the present time to apply those established principles to new situations. Such an approach is indeed possible, as was shown through the example of protecting freedom of speech online; nonetheless the notice and take down procedure in the existing framework does not meet human rights requirements.

4.3. Other human rights aspects of ISP liability

ISP secondary liability regime and the notice and take down procedure, as shown in cases evaluated in other chapters, raise human rights concerns additional to those assessed above. Some may claim that other controversies and issues are far less important, but without doubt all

of them influence ISP liability legal framework established in EU member states compliance with human rights standards.

4.3.1. Legitimacy and accountability

It is often underlined while assessing ISP liability regimes that the entire framework which puts ISPs in a position of control lacks legitimacy and accountability. Any limitation of freedom of expression should be overseen by public law mechanisms and we cannot find such in private terms of service of ISPs, which usually outline the bases for taking down or blocking content. Such legal basis cannot in all certainty be named legislative. Therefore the legal grounds for taking down any content should be provided by states in legislative measures and those principles should be only applied by ISPs. Thus, the current situation is altered and ISPs are empowered to not only to apply regulations, but also to create them.

Lambers has introduced the term of "tilting" into the narrative on ISP liability.[242] His idea is that classical vertical state-individual characteristic of human rights is transformed: the third party – the private entity ISP – has inserted itself between the two parties traditionally involved.

Such a shift is problematic from a perspective of legitimacy and accountability. While the state is bound by constitutional provisions and its actions must always have legal grounds, ISPs, as an examples of private entities, are not subject to the same high standards of judicial scrutiny.[243]Therefore we can observe freedom of expression becoming less protected by constitutional provisions and governed more by private law instead. Of course, there is vivid

[242] Lambers, Rik „Code and speech. Speech Control through network architecture" in: Egberts Dommering and Lodewijk Asscher (eds.) "Coding regulation: Essays in the Normative Role of Information Technology", The Hague, 2006, pp. 115-118.
[243]T.J. McIntyre, „Assessing internet blocking system" in: Ian Brown (ed.) "Research Handbook on Internet Governance", UK, 2013, p.293.

discussion in doctrine whether ISPs should in such situations be perceived as private bodies[244] or entities accountable for human rights violation on the same level as countries.[245] Nevertheless, the problem was also noticed on international political level:

"There is concern that voluntary blocking mechanisms and agreements do not respect due process principles within the states in which they are used. In the absence of a legal basis for blocking access to websites, platforms and Internet content, the compatibility of such agreements and systems with OSCE commitments, Article 19 of the Universal Declaration, Article 19 of the International Covenant on Civil and Political Rights67 and Article 10 of the European Convention on Human Rights is arguably problematic. Although the authorities' good intentions to combat child pornography and other types of illegal content is legitimate, in the absence of a valid legal basis in domestic law for blocking access to websites, the authority or power given to certain organizations and institutions to block, administer and maintain the blacklists remains problematic. Such a 'voluntary interference' might be contradictory to the conclusions of the Final Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE and in breach of Article 19 of the International Covenant on Civil and Political Rights and Article 10 of the European Convention on Human Rights unless the necessity for interference is convincingly established."[246]

4.3.2. Transparency

As reminded in chapter 3, all limitations of freedom of expression, in order to be legitimate, must be prescribed by law.[247] It means e.g. that the legal basis for any interference has to be accessible to public opinion, in this case a wide and diverse assemblage of Internet users.

Many authors, such as Lessig, pointed out that various forms of terms of use (which are usually perceived as a legal basis of notice and take down procedure) are very often not

[244] According to Mueller, such an approach makes it possible for users „to vote with their feet" and once they are not satisfied with the level of fundamental right protection offered by one ISP, they can simply change the company, vide: Mueller, Milton, "Networks and States: the global politics of Internet governance" , Cambridge 2010, p. 61.
[245] Edward on the other hand claims that notice and take down procedure makes ISP accountable the same way public authorities are for human rights violation, Edwards, Lilian, "Pornography, censorship and the Internet", in: Lilian Edwards and Charlotte Waelde (eds.) "Law and the Internet", Oxford, 2009, pp. 45-47.
[246] Akdeniz, Yamanand, „Freedom of expression on the Internet: study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating states", Organization for security and co-operation in Europe, available at: http://www.osce.org/fom/80723, last accessed on 7 November 2013, p.24.
[247] Art. 10(2) of the European Convention of Human Rights.

comprehensible and users are not aware why the content was blocked.[248] Moreover, it is general online habit (part of Internet illiteracy) that users accept terms without reading provisions – nothing surprising in such a "hurried" environment of demand as the Internet. These two factors result in general lack of awareness of what forms of content are prohibited online.

Likewise, traditionally censorship was aimed either a reader or the author of the content. The situation became more complicated online and the way and manner the content is blocked/taken down is sometimes only known to the ISP. Private terms of conditions and the process of drafting are deprived of public attention and scrutiny, which is link to action of judiciary and legislator bodies. The situation was best concluded by Deibert and Villeneuve: "notice and take down (…) is largely new territory, the rules by which states implement such controls are poorly defined, not well known among the general public, and very rarely subject to open debate(…) as it stands now, such decisions are typically taken behind closed doors through administrative fiat".[249] Therefore it is desirable to have more specified legislation on the state's level which is only applied by ISPs - nowadays it is impossible to oblige private entities to take transparency requirement into account while creating terms of use.

4.3.3. Mission Creep[250]

Going back to overall characteristics of the Polish cases from chapter 3, it can be easily recalled that almost all of them referred to political blogs, vivid public debates and burning social issues. Notice and take down procedure was used as a tool in political fights and was a measure

[248] Lessig, Lawrance, "Code: And other laws of cyberspace", New York, 1999, p.153.
[249] Deibert, Ronald Nart Villeneuve "Firewalls and Power: An Overview of Global State Censorship of the Internet" in Mathias Klang and Andrew Murray (eds.), "Human Rights in digital age", London 2009, p. 251.
[250] The term used in McIntyre, "Child Abuse images and Cleanfeeds: Assessing internet blocking system" in: Ian Brown (ed.), "Research Handbook on Internet Governance", UK, 2013, p. 295.

to silence opponents and those holding inconvenient opinions. Therefore ISP liability regime can be claimed to be prone to 'mission creep'. The system established to protects the rights of particularly vulnerable users in the Internet environment can be easily twisted to achieve other, non-human rights related goals.

Taking into account what factors ISPs use to justify blocking content (namely a motivation to be exempted from liability, so simply economic purpose[251]), it is not surprising that insufficient consideration is given to every notice and that perfectly legal content is often blocked or removed, causing collateral damage.

4.4. Conclusions – the future of ISP liability in the European Union

It can surely be claimed that current ISP liability is under constant revision process. The question is, in which direction changes will go. So far, the answer to this question is undefined. We can observe different trends on EU and member states levels which can result in even more discrepancy than we face today. On the other hand, discourse on ISP liability seems to be very limited and narrow-minded due to an unchangeable focus on notice and take down procedure as the only solution possible.

[251] „To protect themselves from sanctions, rather than to protect target from censorship", Kreimer, Seth, "Censorship by Proxy: The first amendment, Internet Intermediaries and the Problem of the Weakest Link", *University of Pennsylvania Law Review*, Vol. 155, No. 11, 2006, p. 36.

4.4.1. The future of ISP liability – ongoing debate on EU level

The EU is aware that something has to be done about ISP liability regime, the way the E-Commerce directive is constructed, and implementation in national legislations. The issue of ISP liability was among the questions asked during public consultation on the Directive held in 2010.[252] It was concluded in the final report that generally the amendment of the legislation is not necessary, but clarification is desirable.[253] It was accentuated by many participants that the notice and take down procedure is necessary to be précised. The stakeholders got to three main conclusions concerning article 14 of the E-Commerce directive: the procedure should result in prompt removal of the infringing content, fundamental rights should be taken into account while creating notice and down procedure, and legal certainty of ISPs should be the ultimate goal of any changes. These demands are absolutely legitimate, but also in my opinion not so easy to be reconciled.

Digital Agenda for Europe, launched by the Commission in 2010, sets its aim as "updating the E-Commerce directive".[254]. Therefore the Commission decided to undertake in-depth studies on the harmonization of the directive's implementation, both from a legislative and case law perspective. The research was planned to be published in the first part of 2013, which did not happen.[255]

[252] Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC), available at: http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm, last accessed on 8 November 2013.
[253]Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf, last accessed on 8 November 2013, pp. 10-15.
[254] Digital Agenda for Europe, Brussels, 26 August 2010, COM(2010) 245 final/2, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=com:2010:0245:fin:en:pdf, last accessed on 8 November 2013.
[255] E-commerce Action plan 2012-2015, State of play 2013, Brussels, 23 April 2013, SWD(2013) 153 final, available at: http://ec.europa.eu/internal_market/e-commerce/docs/communications/130423_report-ecommerce-action-plan_en.pdf, last accessed on 8 November 2013, p. 3.

On 11 January 2012, the Commission announced the communication on a coherent framework for building trust in the Digital Single Market for e-commerce and online services.[256] The notion of "notice and action procedure" was first introduced. As stated in the document:

"The notice and action procedures are those followed by the intermediary internet providers for the purpose of combating illegal content upon receipt of notification. The intermediary may, for example, take down illegal content, block it, or request that it be voluntarily taken down by the persons who posted it online. This initiative should encourage rather than undermine more detailed initiatives in certain fields. For instance, the European Protocol signed in May 2011 between major rights-holders and internet platforms on the online sale of counterfeit products requires, in addition to a notification and take-down procedure, action against repeat infringements as well as proactive and preventive measures."[257]

It must be kept in mind that the commission is not the only actor which is involved in creating EU policy on ISP liability. In December 2011, in the European Parliament, the seminar 'Self-regulation - should online companies police the Internet?' took place. Werner Stengg, the head of Online Services at DG Market in charge of the E-commerce directive review, said to MPs:

*"*We will announce an initiative on notice and action based on the directive. One of the main conclusions is that the directive will not be changed. Articles linked to the liability regime will stay as they are but we will look into the procedures that implement these principles[….]to see if there is any good practice that could be taken as a general guidance on how such a process could be carried out. We are not just talking about economic interests here but very much all the fundamental rights and freedoms that are concerned by this […]*".*[258]

[256] A coherent framework for building trust in the Digital Single Market for e-commerce and online services, Brussels, 11 January 2012, COM(2011) 942 final, available at: http://ec.europa.eu/internal_market/e-commerce/communications/2012/index_en.htm#maincontentSec2, last accessed on 8 November 2013.

[257] A coherent framework for building trust in the Digital Single Market for e-commerce and online services, Brussels, 11 January 2012, COM(2011) 942 final, available at: http://ec.europa.eu/internal_market/e-commerce/communications/2012/index_en.htm#maincontentSec2, last accessed on 8 November 2013, p.13.

[258] The Seminar: "Self"-regulation: Should online companies police the internet?", recording of the live webcast from 7 December 2011, available at: http://www.barouhandpartners.com/livestream/schaake.htm, last accessed on 7 November 2013.

Stengg's communication suggests that there are many subjects interested in ISP liability, fundamental rights get more recognition in the e-commerce, but also there is no specific plan or idea how to approach the issue.

All those measures must be evaluated as positives attempts, but only attempts. The question remains what about their effectiveness and if such non-legislative measures can guarantee the proper protection for freedom of expression and other fundamental rights at stake. Nobody thus far has raised the concern that maybe "notice and action" should be regulated more specifically on the directive level, which will result in creating legal obligation for private entities and better protection of citizens' rights. Such an approach was undertaken in other areas of EU competences[259], but so far nothing gives reason to hope it will likewise be an approach in the e-commerce sector.

4.4.2. The future of ISP liability – ongoing debate in Poland

In Poland, the issue of revision of the E-Services Act has been quite vivid for several years in public debate. A proposal was prepared by the Committee of Ministries and put forward for consultation by civil society, yet not presented in the Parliament.[260] The proposal raises various human rights concerns.

The proposal generally is pro-freedom of expression by giving ISPs less discretion in deciding on freedom of expression of their users by establishing some procedures. It provides specific, separate chapters on notice and take down procedure, including a copy of those

[259] E.g. Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, Official Journal L 303 , 02/12/2000 P. 0016 – 0022.
[260] Ustawa o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz ustawy kodeks cywilny [Revision act of the E-Services Law and the Civil Code], the proposal of 10 November 2011, available at: http://bip.msw.gov.pl/bip/projekty-aktow-prawnyc/2011/20209,dok.html, accessed on 10 September 2013.

provided in the US in the Digital Millennium Copyrights Act. It is worth stating that DMCA is the act regulating only IP infringements, while the Polish legislator wants to apply such framework to all, often various types of infringements. The same procedure will be applied to the situation of defamation and child pornography, which can be questionable. All rights which face infringement online are treated as equal, and a balancing exercise with rights of author of the content was decided to be treated the same way in very various legal situations.

Condensing what information should be given to perceive the notice as "reliable" is a positive step forward in creating more certain legal framework of ISP liability, but still many issues remain unaddressed. Regulation of the procedure is only partial and put stress on the notification, totally disregarding rights of the author of the content. Moreover, the issue discussed in chapter 3, e.g. what "actual knowledge" means, were not solved in the proposal. Alarmingly, there is also a very detailed catalogue of entities that can benefit from legislative safe harbour. Such an approach is reprehensible – the Internet is so rapidly changing that the provisions should be as broad and descriptive as possible, to cover various business models not yet existing. There are also some very progressive legal solutions provided in the proposal, such asthe provision that hyper-links and search engines cannot be subject to any kind of secondary liability (as a reminder, their situation is usually not prescribed by law).

To conclude, debate per se and the idea to amendment existing, not perfect legislation, is worth applauding. But the way the problem is approached, not solving issues which are alarming on the level of judiciary decisions and not giving proper consideration to the issue of human rights aspects of the problem cannot be accepted and need further attention.

4.4.3. The future of ISP liability – possible scenarios

As addressed previously in the thesis, waiving ISP secondary liability in total is not an option.[261] Due to anonymous character of the Internet communication and the scope of other human rights it is necessary to have a system enabling users to protect their rights even if it is impossible to establish who is a really the infringer.

Nevertheless, notice and take down procedure is not the only possible scenario by which to regulate requirements within ISP legislative safe harbour. There are few other scenarios worldwide which address the problem of user generated content and ISP liability. Notice and take down itself can have many various scenarios, with or without procedural guarantees for the author of the content. It is also suggested by some that the person whose rights were infringed should have limited time to start court proceeding against the infringer, and in the case of not taking any legal steps the content should be re-published.

Moreover, there is also a possibility of creating other systems of ISP reaction on notifications, such as[262]:

- notice and notice[263] - ISP in only an intermediary between infringer and person whose rights were infringed and only pass the notice to the author of the content, without revealing his identity;
- notice and stay down – ISP, after taking down of the content, is obliged to monitor if the content is not re-posted by the same user;

[261] But such a solution will be probably enacted in Brazil – legislation work on Marco Civil da Internet is in progress, docket PL 2126/2011.
[262] All those scenarios are mentioned in the report prepared by Szymielewicz, Katarzyna and Anna Mazgal (Panoptykon) "Internet a prawa podstawowe" [Internet and fundamental freedoms], available at: http://wolnyinternet.panoptykon.org/sites/default/files/raport_na_www.pdf, last accessed on 8 November 2013.
[263] The solution discussed e.g. in Canada in the case of IP infringement, in the proposal of the Act to amend the Copyright Act, bill C-60, available at: http://www.parl.gc.ca/HousePublications/Publication.aspx?Doc=C-60_1&Language=E&Mode=1&Parl=38&Pub=Bill&Ses=1, last accessed on 5 September 2013.

- notice and disconnect - in the case of re-posting of infringing content, the ISP has to cut down the service for the specific user.

Unfortunately, the EU and member states are so attached to the idea of notice and take down (in itssimplest and the least prescribed form) as to the only possible scenario that not much attention was given to other legal possibilities so far.

As showed above, ISP liability is without doubt the issue most relevant for human rights protection, especially when freedom of expression is at stake. Various allegations towards the current state of the game can be named, as issues of the rule of law, legal certainty, legitimacy and transparency. The legal framework of ISP liability as constructed nowadays shows an interesting trend of privatization of censorship powers online. Various private entities were given competence to decide not only about freedom of expression, but in the same time put in positions of judges –the system lacksthe mechanisms of public scrutiny or judicial review. Such an approach results in depriving users of procedural guarantees, which was disapproved in March 2008's Recommendation97.[264] The recommendation of the Committee of Ministers is that users should have at least minimal procedural guarantees, such as challenging the decision to take down the content or seek remedies. But the practice can be concluded with the statement of American Civil Liberties Union: "notice and take down procedure violates due process concepts that are also enshrined in international, regional, and national guarantees around the world".[265] Users are deprived of any measures to enforce their freedom of expression, both against public authorities and private actors.

[264] Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters: Adopted by the Committee of Ministers on 26 March, 2008 at the 1022nd meeting of the Ministers' Deputies, available at: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20CMRec(2008)6%20E.pdf, last accessed on 8 November 2013.

[265] American Civil Liberties Union, Press Release, "ACLU Joins International Protest Against

Assessing human rights implications of ISP liability from private censorship and obligations of private entities is certainly a legitimate approach, but still not well established in the literature – the debate is ongoing. Nevertheless, assessing the problem from classic, horizontal approach to human rights citizens-states is probable and appropriate. It should be concluded that nowadays legislation and judicial practice of member states of the EU do not secure enjoyment of right to free speech online. Countries, obliged to comply with both EU obligations of economic nature and human rights standards of the CoE did not establish sufficient safeguards of freedom of expression in ISP liability regime. The lack of specific and certain legislation results in great direction of ISPs and very uncertain legal systems. There is no reason to claim that member states violate a negative aspect of freedom of expression – they are not direct censors of online content. But due to the poor legislation, countries made it possible for other entities to censor online speech, which is a violation of positive aspects of freedom of expression, namely creating proper legal framework.

In my opinion, member states will be in easier legal position to accommodate various international obligation once the E-Commerce directive is more specific and takes into consideration human rights arguments. The EU is not party to the ECHR (yet) and there is no possibility to challenge the E-Directive regulation itself, only its implementation measures. Therefore, ultimately, these are countries that should take appropriate measures to create certain and prescribed legal framework taking into account both human rights and e-commerce development arguments.

Global Internet Censorship Plans," 9 September 1999, available at: https://www.aclu.org/human-rights/aclu-joins-international-protest-against-global-internet-censorship-plans, last accessed on 15 November 2013.

CONCLUSION

We live in the web 2.0 era[266], user movement[267] or read/write culture[268] - the user generated content became dominant online.[269] Consequently the issue who and how an entity can interfere in users' freedom of expressions online is fundamental. The thesis deals with the issue of ISP secondary liability and legislative safe harbour created by the E-Commerce directive. Practice shows that ISPs have extended discretion to decide about the freedom of expression of their users – the member states implemented provisions very vaguely, without providing any details how notice and take down procedure should look like.

Evaluating legislations and judicial cases from different, but interrelated jurisdictions: the EU, the CoE and Poland, revels a series of human rights concerns related to ISP liability. Generally, member states find themselves in the situation of being obliged to implement ISP legislative safe harbour taking into account two various requirements from the EU and CoE. The accommodation of both legal systems in this situation is challenging and therefore the general trend is to leave broad discretion in the hands of ISPs without creating a proper, prescribed legislative framework on the national level.

[266]The term introduced by Tim O'Reilly in "what is Web 2.0", 30 September 2005, available at: http://oreilly.com/web2/archive/what-is-web-20.html, accessed on 10 November 2013. He proposed the shift from platform based and experience-based internet application to integration and interaction based (other name for the phenomena is user movement).
[267]The term introduced by Silke von Lewinsky in "International Copyright Law and Policy",OUP, 2008, pp. 590-593.
[268]The term introduced by Lawrence Lessig in "Remix: Making Art and Commerce Thrive in the Hybrid Economy", Penguin Press HC, 2008, pp.28-29.
[269]Verna, Paul, "A Spotlight on UGC Participants", 19 February 2009, available at:http://www.emarketer.com/Article/Spotlight-on-UGC-Participants/1006914, last accessed on 20 November 2013.

This thesis has shown that member states failed to comply with a positive obligation to protect freedom of expression by undertaking proper legislative measures that will minimize ISPs' discretion impacting freedom of expression of online users.[270]Even without agreeing on the not yet well established horizontal application of human rights, imposing proper legislative framework is a measure which a country can and has to use to secure freedom of expression even online.[271]

The evaluated cases from various jurisdictions show how big a discrepancy exists in applying the same standard within member states, or even the same jurisdiction. To name some human rights concerns evaluated in the thesis, any procedural guarantees for Internet users whose content was taken down, the right to appeal or any procedures of due process have not been secured. Moreover, the ISP liability legal framework is not transparent, sufficiently securing freedom of expression. The existing legislation strengthens private censorship online and is not in accordance with the rule of law, legitimacy, transparency and accountability requirements. To conclude, the current practice and legislation creates an unacceptable situation of legal uncertainty for all stakeholders involved: ISPs, Internet users, and protected rights holders.

Very radical voices in the debate claim that it should never be possible for an ISP to take any content down: "Business operators should never be entrusted with(…) guidelines defining the limits of the right to free speech and offering procedural guarantees against censorship(…)

[270]"It only takes a Hotmail account to bring a website down, and freedom of speech stands no chance in front of the cowboy-style private ISP justice."Nas, Sjoera (Bits of Freedom), "The Multatuli Project: ISP Notice & take down", 1 October 2004, available at: http://www.bof.nl/docs/researchpaperSANE.pdf, last accessed on 20 November 2013.
[271] "In practice positive rights are an important source of indirect horizontal effect. This is because to the extent that constitutional rights require government to regulate private actors, private actors are indirectly affected by and subject to them" - Gardbaum, Stephen "The Stracture and scope of the constitutional rights" in Tom Ginsburd (eds.) "Comparative Constitutional Law (Research Handbooks in Comparative Law Series)" ,Edward Elgar Pub, 2013, p.397.

which belong to the very core of the human tights of democratic people".[272] I do not agree with such a naïve approach – without doubt the Internet works due to the existence of private entities. The challenge for states is to create such legal frameworks which make it possible for ISPs to secure both free speech and other human rights without ISPs being put in the position of pseudo-judiciary bodies. ISPs simply lack knowledge, know-how, the will and competence to decide on human rights issues.

Clearly, there are many legal situations where EU member states' courts decide differently on the same legal issue – but in the case of ISP liability this is especially alarming due to two reasons. Firstly, the Internet is a borderless channel of communication and other liability exemptions cannot be applied in different jurisdictions. It is simply ineffective and can have a "chilling effect" on Internet growth. Additionally, ISP legislative safe harbour, as demonstrated in the thesis, influences freedom of expression protection and it is unacceptable that the standards of protection are so different in various member states.

In my opinion there are two ways to tackle ISP secondary liability to make a legal framework more human rights aware and both need to be implemented simultaneously. Firstly, amendments are needed at national levels of EU Member states. Verbatim implementation of the directive appeared to be insufficient. Moreover, even if the EU is not party to the ECHR yet, it is desirable to introduce legal changes at EU level.[273] Both national and community measures should introduce:

[272] Frydman Benoit and Isabelle Rorive,„Regulating internet content through intermediaries in Europe and the USA", *ZeitschriftfürRechtssoziologie* 23 (2002), issue 1, p.59.

[273] Such a conclusion was also reached by Vaciago, Giuseppe and Silva Ramalho "The Variety of ISP Liabilities in the EU Member states", *Computer Law Review International* 2/2013, p.37 – but they based their conclusion on the principle of free movement of services.

- An open-ended catalogue of ISP being able to benefit from safe harbour. The directive should not be limited to only 3 types of ISP – the current question mark is what about cloud computing, web 2.0 services, web services, wiki's, and content sharing services.
- A harmonized and balanced notice and takedown procedure, with provided procedural guarantees for Internet users.
- A "Put back" procedure is necessary – once the content is taken down without legitimate reasons.
- Very specific language of regulation, with certain and clear definitions.
- Measures to facilitate human-rights oriented self-regulations.

In the literature there are also two other resolutions presented, but I am not persuaded about their feasibility. Some claim that private entities should recognize their role in protection of freedom of expression and decide to be bound by the same high standards as countries[274] – I would love to see this happening, but we cannot expect from entities working for-profit to undertake such commitments on their own. Other authors argue that an international treaty is needed on what ISP secondary liability is, with a clear definition of what it covers[275] - but taking into account current international relations and lack of trust in international organizations I cannot see this happening.

I am well aware that the issue of ISP liability is a broad and complex problem which needs to be evaluated from different, not only freedom of expression, perspectives, such as: technical constrains, business conditionings, data protection, and privacy law enforcement. Moreover, this

[274] Ethan Zuckerman "Intermediary censorship" in: Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.), "Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace", The MIT Press , 2010, p. 83.

[275] Smith, Emerald, "Lord of the Files: International Secondary Liability for Internet Service Providers", W*ashington & Lee Law Review* 68(3), p. 1584.

is a very interrelated issue, unable to be separated from the concerns related to self-regulation online or jurisdiction in the Internet. However, in both political and academic discourses on this issue the role of freedom of expression has been neglected – this thesis shows how significant the freedom of expression perspective is in the discourse on the future of ISP secondary liability in the EU.

BIBLIOGRAPHY

Articles/Books/Reports

1. Akdeniz, Yaman and Horton Rogers, "Defamation on the Internet" in: YamanAkdeniz, Clive Walker and David Wall (eds.), "The Internet, Law and Society", Pearson Education Ltd., 2000
2. Akdeniz, Yaman, "To Block or Not to Block: European Approaches to ContentRegulation, and Implications for Freedom of Expression", *Computer Law and Security Review,* Vol. 26(3), May 2010
3. Akdeniz, Yamanand, „Freedom of expression on the Internet: study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating states", Organization for security and co-operation in Europe, available at: http://www.osce.org/fom/80723
4. American Civil Liberties Union, Press Release, "ACLU Joins International Protest Against
5. Arnull, Anthony, "The European Union and Its Court of Justice", Oxford: Oxford University Press, 2006
6. Balkin, Jack M., "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society", *New York University Law Review,* Vol. 79, No. 1, 2004
7. Balkin, Jack M., "The Future of Free Expression in a Digital Age", Faculty Scholarship Series, 2009
8. Benoit, Frydman and Isabelle Rorive, „Regulating internet content through intermediaries in Europe and the USA", *ZeitschriftfürRechtssoziologie* 23 (2002)/1
9. Bosma, Heleen, "Freedom of Expression in England and Under the ECHR" in Heleen Bosma (ed.) "Search of a Common Ground - a Foundation for the Application of the Human Rights Act 1998 in English Law", Antwerp: Intersentia/Hart, 2000
10. Cheung, Anne and Rolf Weber, "Internet governance and the responsibility of Internet Service Providers", Summer 2008, 26 *Wisconsin International Law Journal* 403
11. Chissick, Michael; "Electronic Commerce: Law and Practice"; Sweet & Maxwell, 2002
12. Christou, George and Semaus Simpson; "The new electronic marketplace: European governance strategies in a globalizing economy"; Edward Elgar Publishing Limited, 2007
13. Clapham, Andrew, "Human Rights Obligations of Non-State Actors", Oxford: Oxford University Press, 2006

14. Cohen-Almagor, Raphael, "Freedom of Expression, Internet Responsibility and Business Ethics: The Yahoo! Saga and Its Aftermath", *Journal of Business Ethics*, 21 July 2011
15. Cucereanu, Dragos, "Aspects of Regulating Freedom of Expression on the Internet", *School of Human Rights Research Series*, V. 27: Antwerp : Intersentia, 2008
16. Deibert, Roland and NartVilleneuve, "Firewalls and Power: An Overview of Global State Censorship of the Internet" in: Matthias Klang and Andrew Murray (eds.), "Human Rights in the Digital Age", London: GlassHouse, 2005
17. Demont-Heinrich, Christof, "Central points of control and surveillance on a "decentralized" Net: Internet service providers, and privacy and freedom of speech online", *Info*, Vol. 4 Issue:4
18. Dijk, Peter and Yutaka Arai, "Theory and Practice of the European Convention on Human Rights", Antwerpen: Intersentia, 2006
19. Dimitris Xenos, "The Positive Obligations of the State under the European Convention of Human Rights", Routledge Research in Human Rights Law, New York: Routledge, 2012
20. Doobay , Dhana; "Google AdWords benefits from E-Commerce hosting defence", available at: http://www.ashurst.com/publication-item.aspx?id_Content=5260
21. Edwards, Lilian, "Pornography, censorship and the Internet", In Lilian Edwards and Charlotte Waelde (eds.) "Law and the Internet", Oxford, 2009
22. Edwards, Lilian, "Defamation and the Internet" in: Lilian Edwards and Charlotte Waelde (eds.) "Law and the Internet : Regulating Cyberspace", Oxford : Hart Publishing, 1997
23. Foley, Conor, "Human Rights and the Internet" in: "Liberating Cyberspace : Civil Liberties, Human Rights, and the Internet" edited by Liberty, Pluto Press, 1999
24. Gardbaum, Stephen "The Structure and scope of the constitutional rights" in Tom Ginsburd (ed.) "Comparative Constitutional Law (Research Handbooks in Comparative Law Series)", Edward Elgar Pub, 2013
25. Garfield, Alan E., "Promises of Silence: Contract Law and Freedom of Speech", *Cornell Law Review*, Vol. 83, 1998
26. Garlicki, Lech, "Relations between Private Actors and the European Convention on Human Rights in The Constitution" in András Sajó and Renáta Uitz (eds.) "Private Relations: Expanding Constitutionalism", Utrecht: Eleven International Publishing, 2005
27. Gerstenberg, Oliver H., "What Constitutions Can Do (but Courts Sometimes Don't): Property, Speech, and the Influence of Constitutional Norms on Private Law", *Canadian Journal of Law and Jurisprudence*, Vol. 17, No. 1, January 2004
28. Gilton, Isabel, "When everything has a price", *Guardian*, 27 August 1996
29. Guillemin, Gabrielle, "European Court strikes a serious blow to free speech online", 14 October 2013, available at: http://www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online
30. Harris, O'Boyle &Warbrick, "Law of the European Convention on Human Right", Oxford University Press, 2009

31. Hosein, Gus, "Open Society and the Internet: Future prospects and Aspirations" in Christian Möller and Arnaud Amouroux (eds.) "The Media Freedom Internet Cookbook", Organization for Security and Co-operation in Europe, 2004
32. Iulia-Barcelo, Rosa and Kamiel Koelman, "Intermediary Liability in the E-commerce directive: So Far so good, but not enough", *Computer Law and Security Report* 2000-4
33. Jakubowicz, Karol, "Media and Democracy", Council of Europe Publishing, Strasbourg, 1998
34. James, Steven, "L'Oréal v eBay & the growing accountability of e-operators" , *e-commerce law & policy*, 2011, volume 13 issue 9
35. Iulia-Barcelo, Rosa, "Online Intermediary Liability Issues: Comparing E.U. and U.S. Legal Frameworks"; *European Intellectual Property Review*, issue 3/2000
36. Konarski, Xawery; „Komentarz do ustawy o świadczeniu usług drogą elektroniczną" [Act on provisions of services by electronic means – commentary], Warszawa, 2004
37. Kot, Dawid; „Dyrektywa Unii Europejskiej o handlu elektronicznym i jej implikacje dla prawa cywilnego" [The E-Commerce Directive and its implications for civil law], *Kwartalnik Prawa Prywatnego*, 1/2001
38. Kreimer, Seth, "Censorship by Proxy: The first amendment, Internet Intermediaries and the Problem of the Weakest Link", *University of Pennsylvania Law Review*, Vol. 155, No. 11, 2006
39. Kuczerawy, Aleksandra; „Odpowiedzialność dostawcy usług internetowych" [ISP liability], available at: http://cbke.prawo.uni.wroc.pl/files/ebiuletyn/Odpowiedzialnosci_dostawcy_uslug_internetowych.pdf
40. La Rue, Frank "The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 16 May 2011, A/HRC/17/27, available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf
41. Lambers, Rik „Code and speech. Speech Control through network architecture" in: Egberts Dommering and Lodewijk Asscher (eds.) "Coding regulation: Essays in the Normative Role of Information Technology", The Hague, 2006,
42. Lessig, Lawrance, "Code: And other laws of cyberspace", New York, 1999
43. Lessig, Lawrence, "Remix: Making Art and Commerce Thrive in the Hybrid Economy", Penguin Press HC, 2008
44. Lewinsky, von Silke, "International Copyright Law and Policy", OUP, 2008
45. Litwiński, Paweł, „Świadczenie usług drogą elektroniczną" [E-services] in: Paweł Podrecki; „Prawo Internetu" [Internet law]; Warszawa 2007
46. Litwiński, Paweł; „Zasady odpowiedzialności pośrednikow w dostarczaniu informacji w internecie" [Rules of liability of ISP]; *Monitor Prawniczy* 24/2002
47. Maclay, Collin, "Protecting Privacy and Expression Online" in Ronald Deibert and Initiative OpenNet (eds.), "Access Controlled : The Shaping of Power, Rights, and Rule in Cyberspace", Cambridge, MIT Press, 2010

48. Mann, Ronald J. and Seth Belzley, "The Promise of Internet Intermediary Liability",*William and Mary Law Review*, Vol. 47, October 2005
49. Margot Horspool and Matthew Humpreys; "European Union law"; Oxford University Press, 2010
50. McIntyre, "Child Abuse images and Cleanfeeds: Assessing internet blocking system" in: Ian Brown (ed.), "Research Handbook on Internet Governance", UK, 2013
51. Medenica, Olivera and Kaiser Wahab "Does liability enhance credibility? Lessons from the DMXA applied to online defamation", 25 *Cardozo Arts & Entertainment Law Journal*
52. Meryem, Mazouki, "The guarantee right for realizing the rule of law" in Rikke Jorgensen (ed.) "Human Rights in the Global Information Society", Information Revolution and Global Politics series. Cambridge and London: MIT Press, 2006
53. Milo, Dario, "Defamation and Freedom of Speech. Oxford", UK: Oxford University Press, 2008
54. Mueller, Milton, "Networks and States: the global politics of Internet governance", Cambridge 2010
55. Nas, Sjoera (Bits of Freedom), "The Multatuli Project: ISP Notice & take down", 1 October 2004, available at: http://www.bof.nl/docs/researchpaperSANE.pdf
56. Newey, Adam, "Freedom of expression: censorship in private hands" in "Liberating Cyberspace : Civil Liberties, Human Rights, and the Internet", Edited by Liberty, London : Pluto Press, 1999
57. Norris, Pippa, "Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide", Cambridge University Press, 2001
58. Nunziato, Dawn, "Procedural Protection for Internet Expression", available at: http://www.osce.org/fom/99458
59. Nyman-Metcalf, Katrin, "Legal Lens: What Delfi v. Estonia Says About Internet Freedom", 14 October 2013, available at: http://www.albanyassociates.com/notebook/2013/10/legal-lens-what-delfi-v-estonia-says-about-internet-freedom/
60. O'Reilly, Tim, "What is Web 2.0", 30 September 2005, available at: http://oreilly.com/web2/archive/what-is-web-20.html
61. Okoń, Zbigniew, "Oskarżony: ISP – odpowiedzialność dostawcy usługi nternetowych" [Accused: ISP – liability of e-services providers], IDG - International Data Group, 1 December 2000, available at: http://www.internetstandard.pl/artykuly/277675/Oskarzony.ISP.odpowiedzialnosc.dostawcy.uslug.internetowych.html
62. Ovey, Clare, Robin C. A. White and Francis Geoffrey Jacobs (eds.), "The European Convention on Human Rights", Oxford : Oxford University Press, 2006

63. Pacek, Grzegorz Jarosław; „Wybrane zagadnienia związane z odpowiedzialnością dostawców usług hostingowych" [Chosen aspects of ISP secondary liability]; *Monitor Prawniczy* 4/2007
64. Pacek, Grzegorz; „Jak należy uregulować odpowiedzialność za treść w Internecie? Wybrane aspekty" [How to regulate ISP liability for USG? Chosen aspects]; article prepared for NGO Panoptykon; available at: *wolnyinternet.panoptykon.org/sites/default/files/pacek.pdf*
65. Perset, Karine (Organization for Economic Cooperation and Development), "The Economic and Social Role of Internet Intermediaries", April 2010, e DSTI/ICCP(2009)9/FINAL, available at: http://www.oecd.org/internet/ieconomy/44949023.pdf
66. Pfanner, Eric; "YouTube can't be liable on copyright, Spain says", *New York Times*; published on 23 September 2010; available at: http://www.nytimes.com/2010/09/24/technology/24google.html
67. Podrecki, Paweł; *„Prawo Internetu"* [Internet law]; Warszawa 2004
68. Reed, Alan "Jurisdiction and choice of law in a borderless electronic environment" in Yaman Akdeniz, Clive Walker and David Wall (eds.) "The Internet, Law and Society", Longman, 2000
69. Reidenberg, Joel "Technology and internet jurisdiction", *University of Pennsylvania Law Review*, 2005 Vol. 153
70. Reidy, Padraig, "European ruling spells trouble for online comment", 11 October 2013, available at: http://www.indexoncensorship.org/2013/10/european-ruling-spells-trouble-online-comment/
71. Rennie, Michèle, "Electronic Commerce: A Review of The European Commission's Proposed Directive", *Computer and Telecommunication Law Review*, 4/1999
72. Report "*European B2C Ecommerce Report 2013" prepared by Ecommerce Europe, available at:* https://www.ecommerce-europe.eu/website/facts-figures/light-version/download%20
73. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee - First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce); COM/2003/0702
74. Robert Uerpmann-Wittzack, "Principles of International Internet Law", 11 *German Law Journal* 1245-1263, 2010
75. Rozakis, Christos, "The Right To A Fair Trial In Civil Cases", *Judicial Studies Institute Journal*, issue 4, 2004, p.7
76. Smith, Emerald, "Lord of the Files: International Secondary Liability for Internet Service Providers", *Washington & Lee Law Review* 68(3)

77. Solove, Daniel J. “The Future of Reputation: Gossip, Rumour, and Privacy on the Internet”, New Haven: Yale University Press, 2007
78. Splinder, Gerard (ed.) “Study on liability of Internet Intermediaries”, 12 November 2007, Markt 2006/09/E, Service Contract ETD/2006/IM/E2/69, available at: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf
79. Staples, William G., “Everyday Surveillance: Vigilance and Visibility in Postmodern Life”, Rowman & Littlefield Publishers, 2000
80. Starr, Sandy, “Putting freedom back on the agenda: why regulations must be opposed at all costs” in: Christiane Hardy and Christian Möller (eds.), “OSCE Spreading the Word on the Internet - 16 Answers to 4 Questions”, available at: http://www.osce.org/fom/13871
81. Sterling, Adrian, “World Copyright Law”; Sweet & Maxwell; 2008
82. Sutter, Gavin “Internet Service Providers Liability”, in: Mathias Klang and Andrew Murray (eds.) “Human Rights in the Digital Age”, London : GlassHouse, 2005
83. Szymielewicz, Katarzyna and Anna Mazgal (Panoptykon) “Internet a prawapodstawowe” [Internet and fundamental freedoms], available at: http://wolnyinternet.panoptykon.org/sites/default/files/raport_na_www.pdf
84. Tambini, Damian, Danilo Leonardi, and Christopher T. Marsden, “Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence”, New York: Routledge, 2008
85. Taylor, Daniel C., “Libel Tourism: Protecting Authors and Preserving Comity”, 99 *Georgetown Law Journal* 189, 2010-2011
86. Uerpmann-Wittzack, Robert, “Principles of International Internet Law,” 11 *German Law Journal*, (2010)
87. Vaciago, Giuseppe and Silva Ramalho “The Variety of ISP Liabilities in the EU Member states”, *Computer Law Review International* 2/2013
88. Van Eecke, Patrick and Maarten Truyens “Liability of online intermediaries “ in: “Legal analysis of a Single Market for the Information Society” (SMART 2007/0037), study of European Commission, available at:http://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037
89. Verna, Paul, “A Spotlight on UGC Participants”, 19 February 2009, available at:http://www.emarketer.com/Article/Spotlight-on-UGC-Participants/1006914
90. Weber, Rolf, “ICT Policies Favouring Human Rights” in: John Lannon and Edward Halpin (eds.) “Human Rights and Information Communication Technologies: Trends and Consequences of Use”, IGI Global, July 2012
91. Wiewiórkowski, Wojciech; “Wyłączenie odpowiedzialności usługodawcy świadczącego usługę drogą elektroniczną za niektóre rodzaje usług” [Exceptions from ISP liability] , *Gdańskie Studia Prawnicze*, issue 21, 2009
92. Ziemele, Ineta, “ Expanding the horizons of human rights law”, The Raoul Wallenberg Institute new authors' series, Leiden, 2005

93. Zuckerman, Etan "Intermidiary censorship" in: Ronald Deibert, John Palfrey, RafalRohozinski, and Jonathan Zittrain (eds.), "Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace", The MIT Press, 2010

Case Law

1. Appelate Court in Kraków (Poland), 19 January 2012, I ACa 1273/11, not published yet
2. Appellate Court in Lublin (Poland), 18 January 2011, I Aca 544/10, published in LEX no 736495
3. Appellate Court in Wrocław (Poland), 15 January 2010, I ACa 1202/09, published in OSAW 2010/2/167
4. Bundesgerichtshof (Germany) , Internet-Versteigerung I, Urt. v. 11 March 2004, Az.: I ZR 304/01 – MMR 2004, 668
5. Court of Appeal of England and Wales, *Tamiz v Google Inc*, [2013] EWCA Civ 68, available at:http://www.bailii.org/ew/cases/EWCA/Civ/2013/68.html
6. Court of Justice of European Union of 12 July 2011; *L'Oréal SA and Others v eBay International AG and Others*; C-324/09
7. Court of Justice of European Union of 23 March 2010; *Google France SARL and Google Inc.v Louis Vuitton Malletier, SA and Others*; Joined Cases C-236/08 to C-238/08
8. Court of Justice of European Union of 26 April 1988, *Bond van Adverteerders and others v The Netherlands State*, case 352/85
9. Court of Justice of European Union of 27 September 1988; *Belgian State v René Humbel and Marie-Thérèse Edel*.; Case 263/86
10. Court of Justice of European Union of 7 December 1993; Stephan *Max Wirth v Landeshauptstadt Hannover*; Case C-109/92
11. Court of Justice of European Union of16 February 2012; *BelgischeVereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*;Case C-360/10
12. District Court in Lublin (Poland), 25 June 2010, I C 618/09, not published yet
13. District Court in Tarnów (Poland), 15 November 2010, I Ns 162/10, not published yet
14. District Court in Tarnów (Poland), 3 October 2011, I C 319/11, not published yet
15. District Court of Hague (The Netherlands - Rechtbank Den Haag), *Scientology v. Providers and others*, 96/1048, 9 June 1999
16. District Court of Wrocław (Poland), I C 625/08, 31 July 2009, not published yet
17. European Court of Human Rights, *Melnychnuk v. Ukraine*, application no, 28743/03, judgment of 5 July 2005
18. European Court of Human Rights, *Brogan and others v. the United Kingdom*, application no. 11209/84; 11234/84; 11266/84; 11386/85, judgment of 29 November 1988
19. European Court of Human Rights, *De Geouffre de la Pradelle v. France*, application no. 12964/87, judgment of 13 December 1991

20. European Court of Human Rights, *Delfi AS v. Estonia*, application no. 64569/09, judgment of 10 October 2013
21. European Court of Human Rights, *Fatullayev v. Azerbaijan*, application no 40984/07 , judgment of 22 April 2010
22. European Court of Human Rights, *Fuentes Bobo v. Spain*, application no. 39293/98, judgment of 29 February 2000
23. European Court of Human Rights, *Golder v. the United Kingdom*, application no, 4451/70, judgment of 21 February 1975
24. European Court of Human Rights, *Goodwin v. the United Kingdom, application* no. 28957/95, judgment of 11 July 2002
25. European Court of Human Rights, *Lombardi Vallauri v. Italy*, application no. 39128/05, judgment of 20 October 2010
26. European Court of Human Rights, *Malone v. the United Kingdom*, application no. 8691/79, judgment of 2 August 1984
27. European Court of Human Rights, *Palomo Sanchez and Others v. Spain*, Application no. 28955/06, 28957/06, 28959/06, 28964/06 , judgment of 12 September 2011
28. European Court of Human Rights, *The Sunday Times v. The United Kingdom*, application No. 6538/74, judgment of 26 April 1979
29. European Court of Human Rights, *The Times v UK*, application no. 3002/03 and 23676/03, judgment of 10 March 2009
30. European Court of Human Rights, *VgTVereingegenTierfabriken v. Switzerland*, application no. 24699/94, judgment of 28 June 2001
31. High Court, Queen's Bench Division (UK),*Godfrey v Demon Internet Service* [2001] QB 201
32. Krakow Regional Court (Poland), I C 1532/09, of 11 March 2010, not published yet
33. Paris Tribunal – Grand Chamber, Bayard Presse v. YouTube LLC, 10 July 2009
34. Paris Tribunal of First Instance (emergency proceedings), *Lambert J-Y ditLafesse v Myspace Inc* 22 June 2007
35. Queen's Bench Division (UK), *Bunt v. Tilley & Others* [2006] EWHC 407 (QB)
36. Supreme Court of Austria, *Online Gästebuch* case, 6 Ob 178/04a
37. The Supreme Court of Poland judgment, IV CSK 665/10, published in OSNC 2012/2/27 and M. Prawn. 2012/10/537-540

Legislation and treaties

1. Belgium - E-Commerce Act of 11 March 2003
2. Estonia - Information Society Services Act of 14 April 2004
3. EU - Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, Official Journal L 303 , 02/12/2000 P. 0016 – 0022
4. EU - 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 July 2000
5. EU - Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations
6. EU - Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Official Journal 217/18
7. EU - Proposal for a European Parliament and Council directive on certain legal aspects of electronic commerce in the internal market; 98/0325 (COD); available at: http://aei.pitt.edu/13258/1/13258.pdf
8. EU - Treaty on the Functioning of the European Union, consolidated version: OJ C 326, 26 October 2012
9. Finland - Act on provision of information society services, 458/2002, 5 June 2002
10. Germany - Das Gesetzüber die Nutzung von Telediensten – Teledienstgesetz, 9020-6 aF, 22 July 1997
11. Italy - Legislative Decree No 70 of 9 April 2003, Decreto Legislativo 9 aprile 2003, n. 70
12. Italy - Ministerial Decree on network blocking of child pornography website, 8 January 2007
13. Lithuania - Law on Information Society Services of the Republic of Lithuania, 25 May 2006, No. X-614
14. Polish Act of 18 July, 2002, on provisions of services by electronic means, official journal no.144, item 1204, as amended
15. Polish Civil Code of 18 May 1964, official journal no 16, item 93, as amended
16. Polish Criminal Code of 6 June 1997, official journal no.88 item 553, as amended
17. Polish Press Law of 26 January 1984, official journal no.5 item 24, as amended
18. Polish Press Law of 26 January 1984, official journal no.5 item 24, as amended
19. Portugal - Decreto-Lei - Law-Decree no 7/2004 of 7 January 2004 on e-commerce
20. Spain - Law of Information Society Services and Electronic Commerce (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, 34/2002, 11 July 2002

21. Sweden - Act on Responsibility for Electronic Bulletin Boards, SFS 1998:112, 12 March 1998, English version available at: http://www.government.se/content/1/c6/02/61/42/43e3b9eb.pdf
22. Treaty on European Union, Official Journal C 115/13
23. UK - Act to amend the law of defamation and to amend the law of limitation with respect to actions for defamation or malicious falsehood, 1996 c 31, available at: http://www.legislation.gov.uk/ukpga/1996/31/contents/enacted
24. UK - Electronic Commerce (EC Directive) Regulations, 2002, SI 2002/2013
25. US - Millennium Digital Copyrights Act, Pub. L. 105-304, 112 Stat. 2860

Other Sources

1. Black's Law Dictionary, Thomson/West, 2005
2. CoE - Declaration of the Committee of Ministers on network neutrality, adopted by the Committee of Ministers on 29 September 2010at the 1094th meeting of the Ministers' Deputies, available at: https://wcd.coe.int/ViewDoc.jsp?id=1678287
3. CoE - Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, adopted by the Committee of Ministers on 26 March, 2008 at the 1022nd meeting of the Ministers' Deputies, available at: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20CMRec(2008)6%20E.pdf
4. CoE - Resolution of the Parliamentary Assembly of the Council of Europe, no. 1877 (2012) on The protection of freedom of expression and information on the Internet and online media, available at: http://assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=18323&Language=en
5. ECtHR - Press release issued by the Registrar of the Court, ECHR 294 (2013), 10 October 2013
6. EU - Illegal and Harmful Content on the Internet, COM (96) 487 of 16 October 1996
7. EU - A European Initiative on Electronic Commerce, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(97)157 of 16 April 1997
8. EU - Coherent framework for building trust in the Digital Single Market for e-commerce and online services, Brussels, 11 January 2012, COM(2011) 942 final, available at: http://ec.europa.eu/internal_market/e-commerce/communications/2012/index_en.htm#maincontentSec2
9. EU - Cohesion and the Information Society, COM (97) 7 of 22 January 1997

10. EU - Digital Agenda for Europe, Brussels, 26 August 2010, COM(2010) 245 final/2, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=com:2010:0245:fin:en:pdf
11. EU - Digital Agenda for Europe, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of 26 August 2010, COM(2010) 245 final/2
12. EU - E-commerce Action plan 2012-2015, State of play 2013, Brussels, 23 April 2013, SWD(2013) 153 final, available at: http://ec.europa.eu/internal_market/e-commerce/docs/communications/130423_report-ecommerce-action-plan_en.pdf
13. EU - EUROPE 2020. A strategy for smart, sustainable and inclusive growth , Communication from the Commission of 3 March 2010, COM(2010) 2020 final
14. EU - European Data Protection Supervisor formal comments on DG MARKT's public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, Brussels, 13 September 2012 available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-09-13_Comments_DG_MARKT_EN.pdf
15. EU - European Union Inter-institutional Agreement on Better Lawmaking, 31 December 2001, Official journal C 321/01
16. EU - Green Papers Living and Working in the Information Society: People First, COM (96) 389 of 24 July 1996
17. EU - Learning in the Information Society - Action Plan for a European Education Initiative, COM (96) 471 of 2 October 1996
18. EU - Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC), available at: http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm
19. EU - Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf
20. EU - Coherent framework to build trust in the Digital single market for e-commerce and online services, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of 11 January 2012, COM(2011) 942
21. EU - The Protection of Minors and Human Dignity in Audiovisual and Information Services, COM (96) 483 of 16 October 1996
22. Organization for Security and Co-operation in Europe, The Representative on Freedom of the Media, "Amsterdam Recommendations on Freedom of the Media and the Internet" from 14 June 2003, available at: http://www.osce.org/fom/13854

23. The Information for Development Program , “The e- Government Handbook For Developing Countries”, available at: http://www.infodev.org/en/Publication.16.html
24. The Seminar: "Self"-regulation: Should online companies police the internet?”, recording of the live webcast from 7 December 2011, available at: http://www.barouhandpartners.com/livestream/schaake.htm
25. UN - Human Rights Committee, “General comment No. 34. Article 19: Freedoms of opinion and expression“,CCPR/C/GC/34, 12 September 2011, available at: http://www2.ohchr.org/english/bodies/hrc/comments.htm, last accessed on 8 November 2013
26. UN - Human Rights Council, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue”, A/HRC/17/27, 16 May 2011, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf
27. Wikipedia, the Free Encyclopaedia, Netizen, http:// en.wikipedia.org/wiki/Netizen