CIVIL LIABILITY OF INTERNET SERVICE PROVIDERS FOR TRANSMITTED INFORMATION: PROBLEMS AND PERSPECTIVES OF LEGAL REGULATION

Karolis Vinciūnas
Vytautas Magnus university
Pateikta 2011 m. lapkričio 5 d.

SUMMARY

With the unprecedented development of the Internet the role of Internet intermediaries that give access to, host, transmit and index content originated by third parties or provide Internet-based services to third parties have grown over the recent years. These entities provide services through both wired and mobile technologies. Internet access intermediaries, hosting and data processing providers create a platform for new, faster and cheaper communication technologies. They also contribute to innovation and productivity gains, provision of new products and services. Furthermore, Internet Service Providers (ISPs) create circumstances for expanding global freedom of expression. However, such a broad proliferation of Internet possesses major threats to privacy protection, copyrights and also helps to spread various sorts of illegal information.

The evaluation of the necessity and scope of the legal responsibility of ISPs for the information transmitted through their networks by third parties and introduction of the conceptual model of mechanisms and principles which could form a background for global unified system of civil liability ascription is the main aim of this article.

In order to achieve this aim, several tasks were formulated and accomplished: firstly, main theories and theoretical approaches of the ISPs civil liability for the information transmitted by third parties were analyzed (Theoretical part of the article, Part I); secondly, factual situation in ISPs civil liability area of EU as a whole, of USA and of Lithuania was presented, the main legal acts were pointed out and the most important cases of this type were examined (Analytical part of the article, Part II); thirdly, main aspects of various legal regimes on which background of the ISPs civil liability system can be built including economic and social implications were singled out; and finally, basic principles for conceptual model of global regime of the ISPs civil liability were introduced (Conceptual part of the article, Part III).

The following methods of theoretical and empirical research were used: 1) comparative research approach; 2) analysis of scientific literature; 3) method of generalization; 4) qualitative analysis.

---

1 Karolis Vinciūnas is a first year PhD student at the Faculty of Law at Vytautas Magnus University. Author’s main area of interest is Internet law and relative judicial processes and jurisprudence around the world. E-mail: karolis.vinciunas@tf.vdu.lt
Based on the analysis conducted in the three different parts of this article, several important conclusions can be drawn and proposals suggested:

1) Theoretical background of the ISPs civil liability, consisting of various liability theories and approaches, is an important part of the new emerging Internet law. Furthermore, its analysis can contribute not only to the better understanding of underlying processes of legal interaction between main actors in cyberspace but also help to construct an analytic framework. This framework would be useful in determining the appropriate scope and under what circumstances and rationale legal responsibility can be ascribed to the ISPs for the actions of third parties. Ascription of legal responsibility to the ISPs for third parties’ actions can be shown as a system of opposing direction of civil liability and regulation processes where regulation and civil liability streams are directed through ISPs accordingly towards end users and initiators of infringements.

2) “The European Community’s Electronic Commerce Directive” (ECD) is one of the main legal acts among other things regulating civil liability of the ISPs in EU. This legislative act uses a mix of contributory and vicarious liability theories and external approach as a background for ascribing legal responsibility to ISPs. Different EU member states interpret provisions of the ECD differently. Such divergent approach determines that courts, who are trying to fill this gap in law system with their decisions, are failing to go along with a pace of Internet technology innovations. This situation reveals an evident lack of unified legislative position in the area discussed. In USA “Digital Millennium Copyright Act” is the main law governing the ISPs civil liability issue and its main difference from ECD is broader rules of exclusion from legal responsibility. This aspect is clearly seen in recent case law of this country.

3) Negligence (notice based) legal regime of the ISPs civil liability is the most popular regime used today. It could become an important part of a possible new global unified system of responsibility ascription, if its main drawbacks – lack of the clear rules of engagement and social-economic inefficiency – are eliminated. Versatile incorporation of Internet freedom, online privacy, internal (technology-friendly) approach, cyber-territorial jurisdiction, consideration of different functioning of various Internet service providers and other principles and their corresponding alignment with the mix of the mentioned legal regimes is probably the best possible solution to sustainable and sound development of the global unified ISPs civil liability system.

KEYWORDS

Internet, Internet law, Internet Service Providers, civil liability.

INTRODUCTION

In recent years as Internet has grown to permeate all aspects of economy and society as well has the role of Internet intermediaries that give access to, host, transmit and index content originated by third parties or provide Internet-based services to third parties increased. They enable to host activities through both wired and increasingly, mobile (wireless) technologies. Internet access intermediaries, hosting and data processing
providers render a platform for new, faster, and cheaper communication technologies, for innovation and productivity gains, and for the provision of new products and services. They also contribute to expanding global freedom of expression.

However, such broad proliferation of Internet poses major threats to privacy protection, copyrights and also helps to spread various sorts of illegal information. Managing responsibility for such actions is one of the major problems which must be dealt with in upcoming years. Also it is one of the corner stones of still emerging Internet law doctrine. Therefore that suppliers and receivers of information are usually hard to trace and prosecute, various Internet Service Providers (ISPs) are the ones who are generally cough up in the center of litigation processes for copyright, privacy or other law infringements taking place in cyber space.

But on the other hand, if ISPs are able to prevent subscribers’ illegal acts cheaply does it mean that they should be ascribed with the costs of preventing the spread of information (or data) infringing various law and if unsuccessful, pay damages and have civil liability imposed on them? These and similar questions must be dealt with and explicit system of ISPs civil liability for third parties’ actions must be created in near future. It is needed in order to ensure the sustainable development not only of Internet law but also of Internet as a whole.

The aim of this article is to evaluate the necessity and scope of the legal responsibility of ISP for the information transmitted through their network by third parties and to introduce conceptual model of mechanisms and principles which could form background for global unified system of civil liability ascription to various actors of online intermediation process.

Main tasks of the article are the following: 1) to analyze theoretical background of the legal responsibility of ISPs and various types of approaches used to apply these theories; 2) to present main legal acts on which civil liability to ISPs for the information transmitted by third parties is ascribed in different parts of the world and to analyze main cases in this area; 3) to present conceptual background for the global model of the ISPs civil liability ascription.

In the first part of the article main theories of the ISPs civil liability for the information transmitted by third parties constitutive, “speech-act”, “respondeat superior”, contributory and vicarious liability are presented and their main aspects are analyzed. Furthermore, prevailing approaches to ISPs responsibility, such as “ex-ante/ex-post”, internal/external or exceptional, are introduced and their impact on ISPs civil liability ascription process is examined. At the end of this part, structural scheme of civil liability/regulation of ISPs is brought and main aspects of overall process are pointed out.

The second part of the article is devoted to presenting factual situation in ISPs civil liability area of EU as a whole, of USA and of Lithuania. The “European Community’s Electronic Commerce Directive” and European Parliament’s resolution “On Cultural Industries in Europe” are examined and their main provisions concerning ISPs responsibility are pointed out. Also implementation of these legal acts in local level is introduced, including case law analysis of France, UK, Belgium courts and European Court of Justice. “Digital Millennium Copyright Act” and “Communication Decency Act” are presented as the main legal acts of USA in the area. Additionally, most important cases
which are forming present *stare decisis* of ISPs civil liability are analyzed. At the end of this part situation of legal ISPs civil liability ascription process in Lithuania is examined and main legislative instruments (including law of electronic communication and decision of government of ISPs responsibility for prohibited information transmission) are presented and relevant ongoing cases in this field are analyzed.

**The third part** of the article is dedicated to presenting the main legal regimes of the ISPs civil liability – negligence (or notice based), strict and non-liability – on which various global legal liability systems can be constructed. Therefore, their main aspects including economic and social implications are pointed out. Finally, basic principles (including Internet freedom and privacy, cyber territorial jurisdiction, etc.) for conceptual model of global regime of ISPs civil liability are introduced.

At the end of the article main conclusions will be drawn and proposals for conceptual background of the legal responsibility of ISPs will be delivered.

In order to achieve the aim of this article, several methods of theoretical and empirical research are used. *Comparative research approach* is used to analyze various legal systems, their main laws and principles, theoretical backgrounds and also their methods to ascribe civil liability to ISPs and to compare different cases of EU, USA and Lithuania in the area discussed. *Analysis of scientific literature* is used to examine main theories and principles of ISP civil liability in order to outline main problems of their practical implementation. *Method of generalization* is used to summarize main findings of analyzed legal framework and cases and to reveal general common principles of ISPs civil liability ascription. *Qualitative analysis method* of case law of European Court of Justice, various EU countries (Belgium, France, UK, Lithuania) and USA is used to assess main principles of certain jurisprudence and outline main patterns in the ISPs civil liability case.

## I. THEORETICAL BACKGROUND OF THE ISPs’ CIVIL LIABILITY

Theoretical background of the ISPs’ civil liability is an important part of the new emerging Internet (cyber) law; its analysis can be useful in constructing various mechanisms for online regulation. Furthermore, it can contribute not only to a better understanding of underlying processes of legal interaction between main actors in cyberspace but also to evaluate certain decisions in various cases in this area around the world. It can be also stated that such analysis can help to structure a conceptual background for the global unified system of civil liability ascription to various ISPs for the third parties action.

The “theoretical basis for ascribing legal responsibility to third parties can be based on that party's constitutive role in enabling illegal acts of others to produce social harm”\(^2\). It is also stated “that the provision by an ISP of access to the enabling technical infrastructure – the network medium – in itself creates a responsibility base for mitigating social harm

---

arising from the use of that infrastructure based on the effects of the mediation in furthering or contributing to the harm”. Such social harm involves illegal dissemination of copyrighted or forbidden material (child pornography and other obscene data, promotion of racial despite or terroristic ideas, etc.), Internet gambling, privacy violations, illegal trade and so forth.

In order to fully understand theoretical background of the ISPs civil liability, firstly ISPs, intermediation process and third parties must be described and their main legal aspects should be pointed out.

1. DEFINITIONS OF ISPS, INTERMEDIATION PROCESS AND THIRD PARTIES

For the purpose of this article ISPs, as mentioned in the introduction, are understood as an entity “that give access to, host, transmit and index content originated by third parties or provide Internet-based services to third parties”\(^3\). ISPs can also be grouped according to functions they execute; that is: 1) Internet access and service providers, 2) data processing and web hosting providers, 3) Internet search engines and portals, 4) e-commerce intermediaries, 5) Internet payment systems, 6) participative networked platforms, etc.\(^4\) It is commonly stated that main functions of these ISPs are the following: “1) to provide infrastructure; 2) to collect, organize and evaluate dispersed information; 3) to facilitate social communication and information exchange; 4) to aggregate supply and demand; 5) to facilitate market processes; 6) to provide trust; and 7) to take into account the needs of both buyers/users and sellers/advertisers”\(^5\). All the before mentioned ISPs differ in their activities, the scope of connection with third parties and information they transmit. Although it is important to assess all of them, because of the limitation of this article only common aspects of their activities and legal nature will be analyzed. It must be stressed that more comprehensive analysis of each kind of ISPs responsibility must be done in other legal research articles in order to fully understand the complexity of the ISPs civil liability.

Intermediation for the purpose of this article can be regarded as “the process by which a firm, acting as the agent of an individual or another firm, leverages its middleman position to foster communication with other agents in the marketplace (Internet space) that will lead to transactions and exchanges that create economic and/or social value”\(^6\). In order to fulfill these functions ISPs have enacted various technical measures which help them to manage intermediation processes; usually under external approach to ISP’s responsibility

---

\(^3\) See id.

\(^4\) OECD’s Committee for Information, Computer and Communications Policy (ICCP) and its working papers provide up to date, comprehensive, systematic and globally accepted assessment of ISPs, their economic and social function, development and prospects, benefits and costs, and responsibilities. For more on economic and social role of ISPs see: K. Perset, “The Economic and Social Role of Internet Intermediaries”, *OECD Digital Economy Papers*, No. 171 (2010), p. 4.

\(^5\) See id.

\(^6\) See id.

\(^7\) Essential part of intermediation is the creation of certain additional value. See *supra note* 4: K. Perset, p. 15.
these technical measures are being analyzed as a primary source for ascribing civil liability to ISPs for the information transmitted by third parties.

Third party (-ies) in the purpose of this article can be regarded as a term for any individual who does not have a direct connection with a legal transaction between ISPs and owners (or beneficiaries) of information but who might be affected by it. Third party concept includes any legal or physical person who is using any services provided by different ISPs and while using them deliberately or not engages in some sort of legal transaction.

After the main terms and concepts used in this article have been introduced, in the next section the theoretical background of the ISPs civil liability for the information transmitted by third parties will be analyzed.

2. THEORETICAL PRECONDITIONS FOR THE ASCRIPTION OF RESPONSIBILITY TO ISPs

It is stated that “the global reach of the Internet, the ease and low marginal cost of replication and transmission of digital data, and the relative anonymity of users have changed the balance of forces that have previously served to keep in check certain undesirable behavior in the physical world.” Thus principles and rules according to which legal responsibility (or liability) to the main actors in cyberspace is ascribed have also changed. In this section of the article main theories of civil liability will be presented and their basic principles will be examined. These theories not only help to better understand the background of the ISPs civil liability but also can be regarded as cornerstones of the global Internet (cyber) law. It must be also pointed out that theoretical basis of the ISPs civil liability for the information transmitted by third parties can contribute to the formation of analytic framework that would be useful in determining the appropriate scope, and under what circumstances and rationale, legal responsibility can be ascribed to ISPs for the actions of third parties.

According to various legal scholars, the following main theories of the ISPs legal responsibility can be singled out – constitutive, “speech-act”, “respondeat superior”, contributory and vicarious liability.

In the next subsections each of the above mentioned theories will be analyzed and their main aspects will be pointed out.

2.1. THEORY OF CONSTITUTIVE (DIRECT) LEGAL RESPONSIBILITY

Meir Dan-Cohen in his book “Harmful Thoughts: Essays on Law, Self and Morality” sets out a theory of responsibility based on what can be called the “constitutive paradigm”.

---

8 Internal and external approaches to ISPs’ civil liability are discussed in chapter 3 of this part of the article. Also see: J. W. PENNEY, “Technology and Judicial Reason: Digital Copyright, Secondary Liability, and the Problem of Perspective”, 22 I.P.J. 251 (2010).
9 See supra note 2: K. A. TAIPALE, p. 4.
10 See supra note 2, 4 and 8.
Usually legal responsibility is based on blame “that is, ascribing moral responsibility for the consequences of one’s actions – are premised on what is generally known as the “free will paradigm” 12. Following this paradigm responsibility is ascribed to a party according to its capacity to decide freely what actions and when can be performed. “Whereas the free will paradigm treats responsibility as a matter of what we choose to do, the constitutive paradigm treats responsibility as a matter of what and who we are.”13 Considering the previous statements, it can be noted that “constitutive responsibility is a function of one’s social “role” in relation to a given action or conduct”14.

In the scope of this article it is very important to analyze the dual structure of constitutive responsibility – that is “object-responsibility” and “subject-responsibility”. “Object-responsibility” relates to direct authorship of an event or behavior while “subject-responsibility” relates to the responsibility base for which object-responsibility may be assigned™15. An example of these two different notions can be an accident brought on by drunk driving: the driver can be ascribed object-responsibility for the accident and/or subject-responsibility for the condition that resulted in the accident, i.e., drunk driving and the responsibility base for attributing object responsibility for the accident is drunk driving.

According to the presented notions of constitutive theory, ISPs can be held liable for their subscribers’ behavior when the former commit infringement (of copyright, etc.) providing basic Internet service to an infringing subscriber; this outcome can seem plausible because ISPs automatically and routinely reproduce and distribute protected (copyrighted, etc.) material in response to subscribers’ requests16. When subscribers upload material to the web pages by instructing the computers of ISPs to make and store a copy of the uploaded material, these “computers make copies of the material every time a person views the subscriber’s web page and send those copies through the Internet to the viewing party”17.

The above mentioned theory was used in USA in early cases18 of copyright infringements on the Internet where liability to ISPs for third parties actions was ascribed because of a mere ability of ISPs to make infringement possible. Such a narrow approach can be regarded as the main drawback of the constitutive theory because “irrelevance of intent or knowledge means that any ISP who reproduces or distributes an article commits

12 See supra note 2: K. A. TAIPALE, p. 5.
13 Responsibility together with ownership is regarded as fundamental concept in interpreting the constitutive role that social practices – particularly law and morality – play in the formation of the self. See supra note 11: M. DAN-COHEN, p. 199 – 200.
14 See supra note 2: K. A. TAIPALE, p. 5.
15 See id.
17 See id., p. 9.
18 Whenever a subscriber downloads information from the Internet his ISP receives copies of copyrighted material and sends that material on to the subscriber. All of this activity arguably infringes the copyright holder’s exclusive rights of reproduction and distribution. See USA case: *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993).
copyright infringement, even when that copying results from the passive execution of subscriber instructions, a practically unlimited scope of liability can soon follow”\textsuperscript{19}. Therefore this theory is not very popular today and is used only as supplementary mean of civil liability ascription to the ISPs.

2.2. “SPEECH-ACT” THEORY

“Speech-act” theory is the analysis of language by what it does through social process rather than what it represents through formal structure\textsuperscript{20}. This theory examines the power of language (spoken as well as written) and how it can be used not only to say something but also to make someone do something. John L. Austin in his book distinguishes language with the primary function of doing something (so called “performative” speech acts) and language used primarily for saying something (so called “constative” speech acts)\textsuperscript{21}. This can be transformed to “the context of cyberspace [where] the information is available on my web site is constative but the statement “<A HREF="http://www.taipale.com/info_here/">Click Here for Information</A>” is performative.”\textsuperscript{22}

It must be noted that the biggest part of legal language is performative because, for example, the phrase “you are negligent” assigns responsibility and has social consequence. Naturally, this aspect of performative speech is very contextual and the above mentioned phrase has a different meaning and understanding weather it is told by someone in the supermarket or by a lawyer in a court. The hyperlink described above “is performative only in context, that is, when embedded in an HTML document”\textsuperscript{23}.

For the purpose of this article the analyzed theory can be enacted when ascribing legal responsibility to the ISPs according to “the relationship of the service provided to the actual harm resulting from the conduct of their users”\textsuperscript{24}. The example of the application of this theory can be the Napster case\textsuperscript{25} where liability to the ISPs was ascribed because it enabled individual user to behave in a way that created or gave effect to the emergence of legal violation.

As previously presented theory of constitutive responsibility, “speech-act” theory also has a pretty narrow approach, especially in the light of recent breakthroughs in online technologies (live video and audio streaming, global social networks, etc.). Almost all ISPs performatively (by helping to transfer information (data) or allowing access to it using

\textsuperscript{20} Under presented theory, words by themselves can create certain acts and this performative ability is very important in analyzing various legal relations on the Internet. For more on performative theory see: J. L. AUSTIN, How to Do Things with Words (Cambridge: Harvard University Press, 1962), p. 6.
\textsuperscript{21} See id.
\textsuperscript{22} See supra note 2: K. A. TAIPALE, p. 20.
\textsuperscript{23} See id.
\textsuperscript{24} See id., p. 21.
\textsuperscript{25} So called Napster case is a landmark intellectual property case in which the United States Court of Appeals for the Ninth Circuit affirmed the ruling of the United States District Court for the Northern District of California, holding that defendant, peer-to-peer file-sharing service Napster, could be held liable for contributory infringement and vicarious infringement of the plaintiffs’ copyrights. This was the first major case to address the application of copyright laws to peer-to-peer file-sharing. See USA case: A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).
mentioned performative language) can be held liable for actions of third parties. Following this it must be stated that it would reasonable to apply this theory in judging the ISPs civil liability only in “mitigating ongoing harm ... either [lack of] actual control or perhaps reckless disregard”.

2.3. DOCTRINE OF “RESPONDEAT SUPERIOR”

Commonly the doctrine of “respondeat superior” is used to ascribe liability to an employer and it is required to show that the conduct in question was within the scope of employment. This theory enacts so called strict liability. Usually it is limited in application because only direct employee/employer (“servant/master”) relationship is needed.

Despite its limitations sometimes the application of this theory can be extended using the so called “abnormally dangerous activity” exclusion. Under this exclusion „strict liability [can be imposed] on abnormally dangerous activities because the risk of harm is great and cannot be eliminated by the exercise of due care”27. As argued earlier, most of activities enabled by ISPs can also be used to make various sorts of violations. Theoretically almost every online activity can be regarded as abnormally dangerous in this sense. On the other hand, technology does not by itself cause an infringement – it is always a physical person who with the help of that technology makes a violation. This can be regarded as the main drawback of the presented theoretical approach.

The other exclusion under which “respondeat superior” theory can be used in the ISPs civil liability cases is that defectively designed products can be held liable for injuries proximately caused by those defects. In this case the factual situation must be analyzed „by comparing the risks and benefits of the product’s actual, allegedly defective design with the risks and benefits associated with an alternate, allegedly non-defective design”28. As it was mentioned earlier, almost all services and products provided by ISPs can be used illegally but it does not mean that all of them have defected design. In order to apply this exclusion, firstly, the actual and potential non-infringing use must be weighted and, secondary, alternate design options must be analyzed29. After combining those results, the overall social value of an actual service or product must be evaluated. If this value is lower than potential harm caused by a service or product, then it can be concluded that it has defective design and ISPs can be held liable for the action of third parties by using this service or product.

This theory in practice is used in those cases when specific technological design of certain ISPs services can be treated as directly injuring interests of some third party and the infringing third party is using those services or products specifically only to implement such actions.

27 Internet technology may be comparable to some sort of abnormal dangerous activity because it creates a significant risk of mass copyright infringement. See: A. C. YEN, ”Sony, Tort Doctrines, and the Puzzle of Peer-to-Peer”, Boston College Law School Faculty Papers, No. 31 (2005), p. 40.
28 See id.
29 See id, p. 41.
30 See supra note 25. See also USA case: In re: Aimster Copyright Litigation, 334 F.3d 643, 654 (7th Cir. 2003).
2.4. THEORY OF CONTRIBUTORY LIABILITY

The theory of contributory liability is best described in USA case *Gershwin Publishing v. Columbia Artists Management*31 where it was stated that “one who, with knowledge of the infringing activity, induces, causes or materially contributes to infringing conduct of another may be held liable as a “contributory” infringer”32. The main aspect of this theory is that it “requires a finding that the defendant’s knowledge and contribution are sufficiently unreasonable to support a particular level of culpability”33. In the ISPs civil responsibility for the actions of third parties case, the level of such knowledge and technological implementation is extremely important when deciding whether to apply contributory theory. On the other hand, the establishment that certain ISPs service or product has the requisites, sufficient to provide knowledge of the infringing activities of its users, usually is complicated because almost every service or product today can be treated as providing enough knowledge to ISPs about its illegal use.

Having in mind this limitation, the new form of contributory liability has emerged. It is called “inducement liability”. In USA case *MGM Studios, Inc. v. Grokster, Ltd*34 Supreme Court stated that “one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement”35. It must be noted that in order to use this kind of liability several points must be proved. Firstly, the aim to satisfy the need of non-legal activity must be shown; secondly, no attempts to develop any filtering tools to monitor or prevent non-legal activity must be made; and thirdly, financial benefit of providing these services or selling products must be proved36. If all these aspects can be proved then contributory (or inducement) liability can be ascribed to certain ISPs for the actions of third parties.

This theory is one of the main used in certain ways in almost all cases of the ISPs civil liability ascription because the nature of ISPs themselves makes ISPs contributory liable theoretically in any legal relationship in which they take any even merely intermediary part.

2.5. THEORY OF VICARIOUS LIABILITY

Vicarious liability is a liability that arises where a defendant has the right and ability to control third party’s infringing activities and where the defendant also receives a direct

---

31 See USA case: *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d1159, 1161 (2d Cir. 1971).
32 See id.
34 Mere knowledge of infringing potential or of actual infringing uses or ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability are not enough to subject a distributor to liability. The inducement rule premises liability on purposeful, culpable expression and conduct that does nothing to compromise legitimate commerce. See USA case: *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).
35 See id.
financial benefit from the infringement. The concept of vicarious liability can also be explained through the “dance hall” and the “landlord” cases. According to those two groups of cases the main factor for applying vicarious liability is scope of control. “Landlords exercise far less control over rented premises than dance hall proprietors do over their halls” and that is why landlords are not being held liable for violations performed by the tenants. Accordingly, it can be summarized that “vicarious liability can be established where the third party has the right and ability to control, and a direct financial interest in the use.” It must be noted that knowledge of the law violating actions is not needed under this theory, so it has a broad application for ISPs civil liability for the services and products provided. Of course, the scope of application depends on the factual situation and today usually ISPs tend to take preventative measures in order to go around this type of liability.

It must be also noted that vicarious liability is sometimes called enterprise liability because under this theory enterprises should internalize losses caused by their existence as a cost of doing business. In our case, ISPs should be ready to accept some part of the damages incurred because of the actions of third parties but it there is a lack of common standard what size of this part must be accepted.

As in previously discussed contributory liability occasion this theory is also broadly used by courts because again the very nature of ISPs can lead to vicarious civil liability for the third parties’ actions using products or services provided by those ISPs.

All the above presented theories form a certain legal background on which different legal systems base their mechanisms of the ISPs civil liability for the actions (information transmitted, etc.) by third parties. In recent years several main approaches of civil liability ascription to ISPs based on the theories described above have emerged. The most important of them will be analyzed in the next section of this part of the article.

### 3. DIFFERENT APPROACHES OF THE CIVIL LIABILITY ASCRIPTION TO ISPS

Different “competing approaches to technology [and thus to liability of ISPs] have deeply influenced judicial reasoning and outcomes in … liability cases,” so it is very important to discuss each of the approaches (“ex-ante” (active-preventative) and “ex-post” (passive-reactive), external and internal, exceptionalistic and non-exceptionalistic) and to point out their main aspects in order to understand their implications in actual legal situations.

---

37 See *id.*, p. 110-111.
38 Dance hall operators are held liable for infringement by bands performing copyrighted articles in their establishments and no liability is imposed on landlords who merely lease space at fixed rates and who have no knowledge or control over the lessee’s infringing activity. These examples can be as well used in analyzing ISPs’ civil liability cases. See *supra note 2*: K. A. TAIPALE, p. 15.
40 See *supra note 2*: K. A. TAIPALE, p. 15.
41 Under enterprise liability theory, ISPs should deter copyright infringement, raise compensation for copyright infringements that occur, and spread costs throughout the Internet-user community. See *supra note 16*: A. C. YEN (2000), p. 11.
42 See *supra note 8*: J. W. PENNEY, p. 2.
3.1. “EX-ANTE” (ACTIVE-PREVENTATIVE) AND “EX-POST” (PASSIVE-REACTIVE) APPROACH

During recent developments of the Internet (and various online activities) different ISPs did not pay enough attention to the fact that much of the third parties’ information (data) was hosted or transmitted by violating certain laws or regulations. “By remaining passive hosts or service providers, ISPs could take advantage of the safe harbor provisions in many jurisdictions’ copyright laws … [which] require intermediaries only to react ex post to notices of infringement.” Such actions grant ISPs immunity from liability for their customers’ (third parties) actions which violate different laws. This so called “ex-post” approach was not only enacted in different laws regulating online activities but was also a favorite approach of the most courts. Under this approach, ISPs are free to provide any services and to sell any products as long as they do not have constructive knowledge that someone is using them to violate existing laws. In this case ISPs are required to “react (in various ways) when they are made aware of the existence of allegedly copyright-infringing material within their system”.

However, in recent years the situation is changing and “entertainment industries, government legislators, and regulatory agencies are increasingly pressuring online intermediaries to take a more active role in preventing copyright infringement with “ex-ante” approach”. Sometimes ISPs are “voluntarily shifting their role from passive providers to active enforcers because they share with some copyright holders a common objective: to become better at proactively managing information transmitted through networks, especially peer-to-peer traffic”.

The result of the collision of these two approaches is changing perspectives to the overall legal liability of ISPs for any actions that take place under their supervision or in cyberspace managed by them. This leads to certain ISPs actions, such as actively policing their networks, filtering content, shaping traffic and otherwise cooperating in cyber-law enforcement efforts.

3.2. EXTERNAL AND INTERNAL APPROACHES

External perspective “approaches the Internet and related technologies from the outside, in technical real terms. The Internet is seen simply as a global information network with users and programmers external to the network and connecting to it with their computers”. External perspective focuses on physical side of the Internet and understands it as a global network “transmitting bits of binary data and other information among end-

44 See id., p. 377.
45 See id., p. 376.
46 While ISPs worry about transmission efficiencies, content owners care more about copyright enforcement. The end result is that both have reasons to support content filtering or traffic-shaping practices. Consequently, many ISPs worldwide began to more actively police their networks, filter content, shape traffic, and otherwise cooperate in copyright enforcement efforts. See id., p. 377.
47 See supra note 8: J. W. PENNEY, p. 2.
users connected by computers”\(^{48}\). This approach was a very important factor in already mentioned USA case *A&M Records v. Napster*\(^{49}\) where external perspective prevailed. The courts in this case agreed that despite *Napster* peer-to-peer file exchange system could also be used in legal way its application in non-legal ways had to be stopped because its operators technically (though practically it was literally impossible) had theoretical possibility to prevent copyright infringements.

“An internal perspective approaches things more from the inside, that is, the way a program or technology defines, affects and limits the experience of users.”\(^{50}\) This approach stresses that “actual technical operations or structure of the Internet has little importance”\(^{51}\) to its legal implications on ISPs. It can be argued that if this approach was used in deciding before mentioned *Napster* case the outcome could have been completely different because under internal approach civil liability of ISPs for the actions (information transmitted) of third parties is limited. It is so because in internal approach users (third parties) are the ones who make actual illegal operations and the mere theoretical technological ability of ISPs to prevent it is not an important factor in deciding liability ascertainment.

Summarizing it can be stated that most probably in the nearest future due to extensive breakthrough in Internet associated technologies internal approach will prevail because only comprehensive treatment of ISPs and their provided services and products can lead to equitable decisions in civil liability cases.

3.3. Approach to the ISPs’ civil liability by Internet exceptionalists and non-exceptionalists

The “fundamental insight [of Internet exceptionalists] is that reliance on local governments to set rules for the new online world would not scale well”\(^{52}\). The alternative they present “is the notion of cyberspace as a separate place which should be ruled by the norms developed by self-governing communities of users”\(^{53}\). On the other hand, Internet non-exceptionalists state that “cyberspace is not a separate place; it is simply a communications network that links real people in real jurisdictions with other people who might be in different jurisdictions”\(^{54}\).

Despite that this approach is more theoretical in its application than the “ex-ante” or “ex-post” approaches analyzed earlier, its implications in today’s legal debates about the ISPs civil liability are very important. It must be particularly stressed that this approach is very important in formation of new laws or regulations concerning ISPs activities and their legal responsibilities. If the approach of Internet exceptionalists prevails then the laws or regulations are not so strict and most of the regulating activities are prescribed to ISPs and other actors of cyberspace. However, if the perspective of non-exceptionalists is treated

---

\(^{48}\) See *id.*, p. 3.

\(^{49}\) See *supra* note 25, USA case: *A&M Records v. Napster*.

\(^{50}\) See *supra* note 8: J. W. PENNEY, p. 2.

\(^{51}\) See *supra* note 8: J. W. PENNEY, p. 4.


\(^{53}\) See *id.*, p. 2.

\(^{54}\) See *id.*, p. 3.
more importantly then the laws or regulations tend to be more rigorous and usually policing powers are prescribed to some governmental institution or organization.

It must be also noted that these different approaches spark debates about a choice whether government should be active or passive in regulating online activities.

The global outcome of this discussion will have huge implications on the ISPs civil liability ascription in the future. All the above mentioned theories and approaches of ISPs responsibility ascription interact with each other and create certain system of civil liability which can be presented in certain schematic way.

4. STRUCTURE OF THE ISPS’ CIVIL LIABILITY ASCRIPTION

As it was mentioned in the previous section of this part of the article, there are several main theories and approaches used to ascribe civil liability to ISPs for the information transmitted by third parties. In order to better understand how the overall process of civil liability ascription is functioning, certain schematic structure can be drawn (see Figure 1).

Figure 1. Structure of the ISPs’ civil liability ascription for the actions by third parties.

As it is illustrated in the figure above, there are opposing directions of civil liability and regulation processes. Civil liability arises from the creators of information (authors, copyright holders, private persons protecting their rights to privacy, other users of ISPs services and products) who are trying to protect their interests by imposing liability first on the consumers of information, then on ISPs and finally on the party who is directly liable for the certain infringement. For example, software development companies tend more usually to sue users who download illegal content than hackers who made that software

55 See id., p. 4.
56 OECD’s ICCP organizes various annual events related between all to the ISPs’ civil liability topics. See: Workshop summary The Role of Internet Intermediaries in Advancing Public Policy Objectives (2010 06 16); <http://www.oecd.org/dataoecd/8/59/45997042.pdf> [visited December 17, 2010].
available online for free. Therefore that third parties and receivers of information usually are physical persons who are hard to find and prosecute, creators of information also tend to sue (or at least include in lawsuits) ISPs for their role in information transmission process. This litigation model is complicated for both – creators of information and ISPs – therefore above mentioned theories and approaches are used to facilitate the desired outcome of the process.

Though, there is process of regulation initiated by supervising institutions (which can be established by certain laws or by private initiatives). Because third parties usually are professional hackers and other advanced users of Internet, supervising bodies focus their actions on receivers of information and on ISPs which can be easily found and sued.

Despite the direction of mentioned processes, ISPs are always in the middle of the structure and therefore usually become first to receive claims of civil liability. To assess how this process is functioning in practice, in the next part of the article situation in the ISPs civil liability area for the information transmitted by third parties in EU and USA will be analyzed and main aspects of its legal implementation will be pointed out.

**II. DIFFERENT APPROACH TO THE RESPONSIBILITY OF ISPs IN LEGAL SYSTEMS AROUND THE WORLD**

The lack of uniform approach, mentioned in the theoretical part of this article, can be clearly seen when analyzing differences in legal acts and jurisprudence in various parts of the world. Legal scholars single out EU and USA as major actors in forming Internet law and concept of ISPs liability as integral part of it. Therefore, in the next sections situation in these two different legal systems will be analyzed more broadly and the main cases in the area will be presented. At the end of this part, Lithuania’s situation will be presented to get a better sense of Internet law perception in newly formed legal systems.

1. EU SITUATION ANALYSIS

1.1. MAIN ASPECTS OF EU E-COMMERCE DIRECTIVE

The main legislative act which is used in EU area to regulate central issues regarding electronic commerce, commercial communications, and formation of online contracts and also liability of Internet intermediaries is “The European Community’s Electronic

---

57 Mere intermediation is still regarded as sufficient background to start litigation processes against ISPs. See: E. D. VENTOSE and J. J. FORRESTER, “Authorization and Infringement of Copyright on the Internet”, 14 No. 6 J. Internet L. 3 (2000).
Commerce Directive” (ECD)59. Several main aspects of this directive concerning liability of ISPs for the information transmitted can be pointed out.

Firstly, according to the article 12 of ECD60, the horizontal exemption from liability for ISPs is established when they play “mere conduit” role in intermediation process of “caching” and hosting information”61. Term “mere conduit” is the cornerstone of this proposition and can be explained through the prism of initiative of ISPs. According to Arno R. Lodder “[ISP] is not liable for the transmitted information only if three conditions are fulfilled: first, the transmission may not be initiated by the provider; second, the provider may not decide to whom the information is sent; third, the provider may not select the information or modify it”62. It must be also noted that horizontal exemption approach is completely different from US law (analyzed in the next section of the article) “under which Internet intermediaries’ liability for third-party content is subject to completely different criteria, depending on whether the liability at issue arises from copyright infringement or from other types of unlawful content”63.

Secondly, according to various scholars64 this act can be treated as an ex-post (passive-reactive) model for dealing with the ISPs civil liability. The ECD “does not impose liability on the ISPs if it does not modify information transmitted by third parties, unless the ISPs acquires actual or constructive notice of illegal content and fails to take prompt remedial steps”65. ISPs “have to remove the information as soon as they know that the initial source of the information is removed, access to it has been disabled, or court administrative authority have ordered such removal or disablement”66. On the one hand, erection of such safe harbors helps ISPs arrange their activities and avoid unnecessary problems concerning liability for the information transmitted. On the other hand, it does not preclude possibility of injunctive relief against a qualifying service provider67.

Article 45 of the ECD provides the possibility of injunctions of different kinds in case termination of certain illegal activity is expeditiously necessary68.

60 The Directive establishes a horizontal exemption from liability for ISP when they play a technical role as a “mere conduit” of third party information and limits service providers’ liability for the other intermediary activities of “caching” and hosting information. See supra note 59: ECD, art. 12.
61 See supra note 4: K. Perset, p. 11.
64 See supra note 16: A. C. Yen (2000) and supra note 52: M. MacCarthy and 58: M. S. Garcia.
65 Almost absolute immunity enjoyed by American ISPs (this topic is present in the next chapter of this part) has the virtue of drawing a clear line that eliminates any exposure to liability for third party content and contrary the imposition of even a limited duty for ISPs creates legal uncertainties and new financial burdens. See: M. L. Rustad and Th. Koengk, “Rebooting Cybertort Law”; 80 Wash. L. Rev. 2 (2005), p. 393. See also supra note 59: ECD, Art. 13 and 14.
67 See supra note 59: ECD, Art. 14, s. 3.
68 The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of
It must be also pointed out that such possibility “creates legal uncertainties and new financial burdens for ISPs – [a need] to bear the expenditures of investigating complaints, tracking down wrongdoers, and making nuanced takedown and put-back decisions under European law”\(^69\). Finally it can be noted that already mentioned lack of uniform approach to this problem by the courts of different EU member states creates hardships to global operations of ISPs who have to adjust their services and products in each EU country according to the legal approach adopted in domestic courts.

Thirdly, ECD points out that there is no general obligation to engage in monitoring activity\(^70\). It is stated “that no general obligation exists for service providers to monitor information they transmit or store; a general obligation to actively seek facts or situations indicating illegal activity does not exist either”\(^71\). This is a very important rule as it does not impose a “cyber police” functions on ISPs and leaves this field to various governmental agents. Nonetheless two exceptions exist to this general rule: first, EU member states may establish obligations on ISPs to inform the authorities of alleged illegal activities or illegal information provided by recipients as soon as the provider becomes aware of it; second, EU member states may also establish obligations on providers to disclose the identity of recipients with whom they have storage agreements\(^72\).

Fourthly, “the ECD’s recitals note that the free development and circulation of information services throughout the European Community is guaranteed by the basic principle of freedom of expression, as set forth in the Article 10(1) of the “European Convention for the Protection of Human Rights and Fundamental Freedoms”\(^73\). This approach sometimes is challenged as it is noted that “[ECD] is being criticized for promoting self-censorship, the loss of privacy, and a decline in the free flow of information”\(^74\). It is hard to find correct answer whether ECD is a sufficient tool to regulate civil liability of ISPs and often approaches (or perspectives) presented earlier in this article must be taken as the main factor for decision making.

\(^69\) It is stated that all and any obligations for ISPs to perform a role of cyber-patrol in order to evade possibility of injunctions come at certain costs which are passed on to computer users and other consumers in Internet access charges. See supra note 65: M. L. RUSTAD and Th. KOENIG, p. 394.

\(^70\) See supra note 59: ECD, Art. 15.

\(^71\) See supra note 62: A. R. LODDER, p. 89.

\(^72\) Such exceptions provide a possibility for any member state impose certain obligations on ISPs. Sometimes these obligations can be regarded as infringing notions of “safe harbor” provided in other cited articles of ECD. See supra note 59: ECD, Art. 15, s. 2.


\(^74\) The absence of comprehensive and universal methods of evaluation of the scope necessary to ensure desired level of online regulation is one of the main obstacles preventing from creating sound and clear system of possible injunctions and thus explicit mechanism of ISPs’ responsibilities. See supra note 65: M. L. RUSTAD and Th. KOENIG, p. 394.
1.2. MAIN ASPECTS OF THE EUROPEAN PARLIAMENT RESOLUTION75 CONCERNING THE ISPS’ CIVIL LIABILITY

As it will be shown later in the article, different states within the EU have adopted different approaches to ISPs civil liability for third parties action. Because of such a broad interpretation of ECD European Parliament (EP) in 2008 adopted resolution “On Cultural Industries in Europe”. In this resolution EP called against policies that would terminate Internet service to repeat infringers and urged European nations to reject France’s example which will be analyzed later in this article. The resolution requires member states to avoid adopting measures conflicting with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of Internet access.76 In resolution it is as well noted that “in the interest of a balance between the opportunities for access to cultural events and content and intellectual property that guarantee fair, effective remuneration to all categories of right holders, real choice for consumers, and cultural diversity”77.

It must be also mentioned that the resolution includes a notion which emphasizes the importance of online access to various cultural material and that “the security of unimpeded access to online cultural content and to the diversity of cultural expressions (must be) over and above that which is driven by industrial and commercial logic, ensuring moreover, fair remuneration for all categories of right holders”78.

All the above outlined statements of the EP’s resolution “On Cultural Industries in Europe” mean that for the moment EU member states do not have a single approach to the problem of the ISPs civil liability. The lack of rules in this area is becoming an increasing problem not only for ISPs but also for the users and all other parties (governments, courts, protectors of intellectual property, etc.) involved in various legal online activities and its regulations.

1.3. ANALYSIS OF THE MAIN CASES OF THE ISPs CIVIL LIABILITY IN DIFFERENT EU MEMBER STATES AND IN ECJ JURISPRUDENCE

Diverse understanding of ISPs civil liability leads to different judicial decisions in the EU on the subject matter. Various cases in which different types of ISPs are being sued for actions of third parties show a broad and unequal application of ECD provisions in almost identical situations.

75 The need to modernize ECD and create new comprehensive on-line regulation can be regarded as an important trend in various recent EU legislative actions in the field. See: European Parliament resolution of 10 April 2008 on cultural industries in Europe, 2007/2153 (INI), 2008.
76 The importance of sustainable Internet development and need to assure its universal and unimpeded accessibility is usually presented as one of the main arguments to reduce the level of ISPs’ civil liability. See supra note 43: J. de Beer and Ch. D. Clemmer, p. 390.
77 See supra note 75: European Parliament resolution, p. 8.
78 See id, p. 8.
1.3.1. FRENCH, BELGIUM AND UK APPROACH TO THE ISPS CIVIL LIABILITY

In the case Lafesse v. MySpace (2006)\textsuperscript{79}, French humorist Lafesse filed a suit against MySpace\textsuperscript{80}, claiming infringement of his author’s rights and personality rights after several videos of his skits appeared on MySpace web site. France’s “Digital Economy Law”\textsuperscript{81} (adopted in accordance with Article 14 of ECD) provides that hosts may not be held civilly liable for the activities or information stored at the request of a recipient of these services “if they did not have actual knowledge of their unlawful nature or of facts and circumstances making this nature apparent, or if, as soon as they obtained such knowledge, they acted expeditiously to remove or to disable access to these data”\textsuperscript{82}. It also stipulates that providers are under no general obligation to monitor the information that they transmit or store. MySpace, having complied with the legislation, should have been protected from such a suit but the Paris Tribunal de Grande Instance (TGI) held MySpace to be the publisher rather than the host of the content. The Paris TGI justified its decision by citing the fact that MySpace allows users to upload content through a specific frame structure. It was also noted that every time the video was viewed an advertisement was displayed and that resulted in advertising revenue for MySpace. Because the court was convinced that MySpace was the publisher it was not permitted to rely on the French hosting exemption (as noted earlier)\textsuperscript{83}.

In the light of the before presented theories and approaches to the ISPs civil liability, it can be stressed that despite actual law being more “ex-post” (passive-reactive) character, the court basically relied on an external approach. By stating that MySpace theoretically could be viewed as a publisher the court focused on the technological side of the case where the mere possibility of MySpace to contribute to copyright violation done by third party was seen as its fault. However, this case can be seen as an example of practice of the vicarious liability theory because MySpace had possibility to control third parties’ actions (by removing infringing content) and also had direct financial interest from infringing activity (advertising revenues).

In another case (Nord-Ouest Production v. Dailymotion (2007)\textsuperscript{84}) Nord-Ouest Production sued the hosting site Dailymotion\textsuperscript{85} after a copy of its film Joyeux Noel

\textsuperscript{80} MySpace is a social networking website, offering its users variety of services, including exchange of messages, pictures, videos and other user modified private information.
\textsuperscript{83} MySpace was ordered to remove the infringing content or face a daily EUR 1,000 fine and to pay EUR 61,000 for commercial prejudice, infringement of moral and personal rights, and the plaintiff’s legal fees. See supra note 79.
\textsuperscript{85} DailyMotion.com is a video sharing service website, allowing its users to share online free of cost various types of video data.
appeared on Dailymotion’s web site without authorization. Dailymotion argued that under France’s “Digital Economy Law” and provisions of Article 15 of the ECD they had no general obligation to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating unlawful activity. The plaintiff argued that Dailymotion was a publisher and as was held in before mentioned case of MySpace and thus must prevent all acts of infringement from occurring. The court held that Dailymotion had deliberately enabled mass-scale piracy because its web site infrastructure was built in first place for sharing not homemade videos but copyright protected data. In contradiction to the MySpace decision, the court held that because Dailymotion did not control the content of the postings they were not a publisher despite the presence of paid advertisements. This can be seen as an example of internal approach to the ISPs civil liability for the information transmitted by third party. If court used external approach to base its decision, the outcome of this part of the case would have been completely different and Dailymotion would be held liable. At the end court held that Dailymotion was nonetheless liable, as the exemption from a general duty to monitor their network did not apply when the unlawful activities were generated or induced by the service provider itself.

Dailymotion was a hosting service provider, and because it must have been aware that its platform was being used for copyright infringement (in fact, it “enabled, induced and thrived on” the induced infringements), it had an obligation to implement technical solutions to prevent all unlawful activities. This approach of the court was based on secondary liability (contributory and vicarious) theories and also showed that courts were not ready to fully accept internal approach to the ISPs civil liability. The Dailymotion ruling expanded the circumstances under which hosting service providers in France could be held liable for infringement. Following the decision, hosting service providers could see their safe harbor protection in France disappear if a court decides they must have been aware of the infringing content, they induced the infringement in an effort to increase traffic to their site, or they profited from the infringement by posting advertisements alongside videos on their Web site.

In Belgium, courts came up even with the stricter standard for ISPs behavior on the subject matter. In the case SABAM v. Scarlet (2007) the collective society representing composers and music publishers in Belgium, SABAM, filed a lawsuit against an intermediary to compel the intermediary to adopt technological measures to stop its subscribers from downloading illegal music. The court ruled that ISPs have both a legal responsibility and the technical ability to stop copyright infringement, and ordered Scarlet to use one of methods suggested in an expert report to either block or filter “p2p” infringements on its network. If Scarlet failed to do this within six months, it was to face a daily penalty. This decision is controversial for at least two reasons. “First, it represents the

---

86 See supra note 82: N. JONDET, p. 5.  
87 Dailymotion was fined EUR 23,000 in damages and a further EUR 1,500 for each day the infringing video stayed online. See supra note 84.  
89 See Belgium case: SABAM v. S.A. Tiscali (Scarlet), Tribunal de Première Instance de Bruxelles (June 29, 2007; No. 04/8975/A).
first time in Europe that such an obligation has been imposed on carriers; second, the judgment appears to contradict a prohibition on monitoring obligations contained in the ECD.\(^90\) Again it can be noted that courts used a completely external approach to the ISPs civil liability and despite that law regulating this area is “ex-post” (passive-reactive) in nature they still held that mere possibility to contribute to infringement can be enough to prove ISPs’ guilt.

Different approach in similar situation was taken by judicial system of UK. In the case\(^91\) against TV-Links\(^92\) it was stated that if ISPs acts only as an indiscriminate conduit to content searched by users, it cannot be held liable for the information transmitted through its network by third parties. On one side, this holding can be viewed as based on an internal approach to the ISPs civil liability. On the other side, it must be indicated that TV-Links engaged in linking activity and thus its exemption due to mere conduit clause in the ECD and its implementation in UK law\(^93\) can seem doubtful. It will probably have no global impact on the topic of the ISPs civil liability, having in mind the Pirate Bay case in Sweden\(^94\) where both lower and appellate courts found ISPs (in this case website’s www.piratebay.org redactors and owners, physical persons) guilty for allowing its customers to share copyrighted content using their website’s infrastructure.

In the other UK case Godfrey v. Demon\(^95\) the plaintiff was a physics lecturer falsely identified as the author of an allegedly defamatory Internet posting. The plaintiff notified the ISP of the postings and requested that they be removed. Demon declined to remove the posting until it expired two weeks and plaintiff sued Demon for spreading defamatory content. The court ruled that “since the plaintiff had notified Demon of the allegedly

\(^{90}\) This decision can be regarded as representing a significant departure from the principle that connectivity providers are “mere conduits”. It also shows that current legislation under ECD is not comprehensive and major gaps are left allowing national courts to interpret certain provisions in a way contravening overall attitude of the ECD. See supra note 43: J. DE BEER AND CH. D. CLEMMER, p. 401.

\(^{91}\) The actual knowledge must be proved in order to obtain injunction and block certain Internet site accused of copyright infringements. Otherwise the provisions of “safe harbor” provided in ECD are employed and ISP is considered as “mere conduit”. See UK case: Rock, Overton v. F.A.C.T., [2010] 4 All Er 121.

\(^{92}\) TV-Links was a UK-based site which linked to movies and TV shows hosted on the other sites as YouTube, MySpace Video or DailyMotion.

\(^{93}\) Despite mentioned TV – Links case ruling present legislation in UK allows copyright holders or other injured third parties seek injunctions and blocking of certain Internet sites. ISPs can be ordered to engage in filtering and blocking activities and bear some of costs related to such activities. See: Digital Economy Act of UK 2010 (c. 24, April 8, 2010).

\(^{94}\) The Pirate Bay case was criminal proceedings against four owners of Internet site www.piratebay.org which was (and in fact still remains) one of the main on-line resource for p2p file sharing links (most of the links are related to copyright protected content). The purpose of the trial was to determine if the mentioned site and its owners promoted copyright infringement with its actions as a torrent tracking website. In the first instance the owners were found guilty of assistance to copyright infringement and sentenced to one year in prison and payment of a fine of $ 3,620,000. Appellate court withheld the decision. The main arguments used by courts were that site owners have the constructive knowledge of continuous copyright infringements and that they did not take any steps to stop such actions and in some instances induced them. See Sweden case: Holding of Appellate Court of Sweden (November 26, 2010; No. B 4041-09).

defamatory content, Demon could not raise the innocent dissemination defense\(^\text{96}\). Despite the negative outcome for ISP because of the lack of timely response in this case, court again used an internal approach to the ISPs civil liability and completely relied on safe harbor provisions, stated in the ECD and its “ex-post” nature regulations.

### 1.3.2 Decisions of ECJ in the ISPs’ Civil Liability Cases

One of the main cases of the ISPs responsibility in European Court of Justice (ECJ) jurisprudence is a case Promusicae\(^\text{97}\) v. Telefonica Spain\(^\text{98}\). In this case Promusicae asked for Telefonica to be ordered to disclose the identities and physical addresses of certain persons whom it provided with Internet access services, whose IP address and date and time of connection were known. Telefonica refused to do it and Promusicae sued it. ECJ held that the ECD “does not require the member states to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings”\(^\text{99}\). This judgment “confirms the relevance to Community law of the fundamental rights, whose balancing becomes a singular principle of interpreting European and national law”\(^\text{100}\). It must be also stressed that such argumentation of the court confirmed main approach used in the ECD – ISPs are not liable for third parties’ actions if they act as mere intermediaries (and that is why in Promusicae case Telefonica was not obliged to provide personal data of its users).

In another ECJ case Vuitton v. Google\(^\text{101}\) Vuitton\(^\text{102}\) sued Google for its users’ actions. Vuitton stated that search results in Google were presented in such manner that ordinary user was unwillingly directed to Internet site that sold unauthorized copies of Vuitton production and so its copyrights were infringed. ECJ held that “[ISP] cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser’s activities, it failed to act expeditiously to remove or to disable access to the data concerned”\(^\text{103}\). With this holding ECJ followed the main theme of the ECD and its ISPs safe harbors rules when no direct control over the data transmitted through their networks exists.

In summary, in different EU countries the interpretations of the provisions of the ECD are different. Such a divergent approach remains a big problem not only for ISPs but also for various governmental institutions responsible for the supervision of cyber space. On one

---


\(^\text{97}\) Promusicae is a Spanish non-profit-making organization of producers and publishers of musical and audiovisual recordings.

\(^\text{98}\) See case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU [2006] ECR I-00271.

\(^\text{99}\) See id.

\(^\text{100}\) See supra note 58, M. S. GARCÍA, p. 191.

\(^\text{101}\) See case C-236/08 joined with C-237/08 and C-238/08, Google France SARL, Google Inc. v Louis Vuitton Malleier SA and others [2010] ECR I-00000.

\(^\text{102}\) Vuitton, which markets, in particular, luxury bags and other leather goods, is the proprietor of the Community trade mark ‘Vuitton’ and of the French national trade marks ‘Louis Vuitton’ and ‘LV’.

\(^\text{103}\) See supra note 101; Case C-236/08 and others.
side, ISPs are having difficulties in adapting to diverse legal approaches in the EU area; on the other, courts are trying to fill this gap in law system with their decisions but the pace of technological innovations makes these tasks very complicated. In the next section of the article another legal regime of the ISPs civil responsibility in USA will be presented and main cases in the area will be pointed out.

2. USA SITUATION ANALYSIS

2.1. ANALYSIS OF THE “DIGITAL MILLENNIUM COPYRIGHT ACT”

Main legislative document which is used to ascribe civil liability to ISPs in USA is the “Digital Millennium Copyright Act” (DMCA). It must be noted that its primary function is to deal with copyright infringements, therefore in the next subsection of this article the “Communications Decency Act” (CDA) will be analyzed in the scope of the ISPs civil liability for unlawful data other than intellectual transmission by third parties. Title II of the DMCA (now codified at Section 512 of the Copyright Act), specifically addresses the issue of the ISPs civil liability for subscriber’s infringement. The DMCA “affects ISPs liability by insulating ISPs from liability as long as they comply with certain statutory requirements designed to facilitate content providers’ efforts to protect their copyrighted material”.

The statute clearly states that these safe harbors do not affect the viability of any other legal grounds on which ISPs might claim non liability. According to DMCA ISPs cannot be held liable when it does not have actual knowledge of the infringement, does not receive financial benefit and acts as requested when the fact of infringement is duly presented and proved.

It must be stated that “all three requirements must be satisfied for the safe harbor to apply”. If the ISP gains knowledge or awareness of infringing activity no liability attaches as long as the ISP removes or disables access to the alleged infringement. All mentioned provisions are basically similar to provisions of then ECD and the biggest difference of these two legal acts is the possibility of injunctive reliefs. As it was mentioned before, the European safe harbors do not limit possibility of injunctive relief against a qualifying service provider. Contrary, the DMCA allows such measure of litigation only

---

105 See supra note 16: A. C. Yeš, p. 45.
106 It is stated that ISPs cannot be ascribed with the responsibility if: (A) (i) does not have actual knowledge that the material or an activity ... is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (B) does not receive a financial benefit directly attributable to the infringing activity, ... [where] the service provider has the right and ability to control such activity; and (C) upon notification of claimed infringement … responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity”. See supra note 104: DMCA, s. 512.
107 See supra note 16: A. C. Yeš, p. 45.
after carefully considering the need, costs and expected results (benefits) of such measure.\footnote{Injunctions are not allowed in case “it [would] significantly burden either the provider or the operation of the provider’s system or network; the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement; whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to non-infringing material at other online locations; and whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available”. See supra note 104: DMCA, s. 512.}

The existence of such limitation is a very important factor of the DMCA because it shows the unwillingness of the government to engage into detailed regulation of cyber space and thus it can be noted that such approach is an example of exceptionalistic approach, mentioned in this article previously.

The other important distinction between usual perception of the ECD in different states and the DMCA application in USA can be made when analyzing the so called constructive knowledge rule. “The constructive knowledge rule assumes that a reasonable ISPs should have known about objectionable content and in effect, dictates the monitoring of all content on its services.”\footnote{See supra note 65: M. L. RUSTAD AND T.H. KOENIG, p. 389} In Europe courts usually tend to apply constructive knowledge rule to actions of ISPs and hold them liable just for mere knowledge of possible law infringement in their networks. In USA such rule is not recognized not only because of the language of the DMCA but also because “this inflexible standard would have a chilling effect on free expression by causing some ISP to shut down their services and by increasing the cost of Internet communications.”\footnote{See id.}

Finally, it must be also noted that in USA the ISPs civil liability for the information transmitted by third parties is broadly affected by the First Amendment\footnote{The First Amendment to the United States Constitution is part of the Bill of Rights. The amendment prohibits the making of any law respecting an establishment of religion, impeding the free exercise of religion, infringing on the freedom of speech and press, interfering with the right to peaceably assemble or prohibiting government critic. The First Amendment and its case law can be regarded as certain set of methodology used to distinguish between necessary and allowed on-line regulation and a free and unimpeded flow of information. See: F. A. PASQUALE, “Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries”, 104 Nw. U. L. Rev. 105 (2010), p. 108.} notions. As it is stated, application of the First Amendment rules in the ISPs civil liability cases must „recognize as protected each of the steps involved in the communicative relationship between speaker and listener ... the right to speak and the right to hear, but also the right to reach an audience free from the influence of extraneous criteria”\footnote{See supra note 65: M. L. RUSTAD AND T.H. KOENIG, p. 389}. The application of the First Amendment rules in courts of USA are very broad and, as it will be shown later in this article, usually this overwhelms basic global principles and approaches of cyber law presented earlier.
2.2. ANALYSIS OF THE “COMMUNICATIONS DECENCY ACT”

Another important USA legislation act that regulates liability of ISP for the information transmitted is the CDA\(^{113}\) which was enacted few years ago before the DMCA. The CDA established “a single bright-line rule [that] no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider”\(^{114}\). Such immunity covers almost all the content excluding from its scope only some criminal law aspects and privacy regulations. On the one hand, this safe harbor helps ISPs avoid unnecessary litigations but, on the other hand, it “limits incentives for intermediaries to take initiatives to censor material passing through their facilities”\(^{115}\). It must be also noted that such almost absolute immunity in certain cases is not consistent with today’s “explosive” usage of Internet and in the near future it should pass extensive review.

In the next subsection of this article main cases in USA related to the civil liability of ISPs will be analyzed and basic notions that courts adopted in these litigations will be presented.

2.3. ANALYSIS OF THE MAIN CASES OF THE ISPs CIVIL LIABILITY IN USA

The first and most notorious case was A&M Records, Inc. v. Napster, Inc.\(^{116}\) and it involved Napster\(^{117}\) whose business model involved possibility to circumvent the copyright laws. In this case court held that Napster was contributory and vicariously liable for the information transmitted by third parties. Court stated that Napster had both actual and constructive knowledge of its users’ infringing activities. The defendants had given Napster plenty of knowledge of the actual infringing files. Further the court also held that vicarious liability was applicable because a sufficient financial benefit related to the infringement occurred where the availability of infringing material acted as bait for customers. Additionally, Napster was found to have the ability to supervise the infringing activities of its customers because it was able to monitor the titles of files traded through its services, even though it did not maintain copies of those files on its own servers\(^{118}\). It can be stated that one of the main aspects of this case is the departure of the court from Sony\(^{119}\) case rules. Because of its online peculiarity “the court distinguished Sony because the ongoing central indexing function gave Napster unlike Sony actual, specific knowledge of direct


\(^{114}\) See supra note 63: M. PEGUERA, p. 484.

\(^{115}\) See supra note 112: F. A. PASQUALE, p. 191.


\(^{117}\) Napster was the first globally known peer-to-peer file sharing Internet service which allowed its users to share audio files that were typically digitally encoded music as MP3 format files.

\(^{118}\) See supra note 36: J. D. LIPTON, p.119.

\(^{119}\) It was ruled that making of individual copies of television shows for purposes of time-shifting does not constitute copyright infringement and that the manufacturers of such video recording devices are not held liable for infringement. See USA case: Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).
infringement by users of its system”\(^{120}\). This was a very important finding which showed that courts are eager to use exceptionalistic approach to the ISPs civil liability issues. In this case court also „did find “real world” precedent for the proposition that financial benefit may be made out where the availability of infringing material in a physical venue acts as a draw for customers, and thus enhances the profits the venue operator may make from charging rents to vendors”\(^{121}\). This type of approach is also very beneficial because courts treat cyber space more as an extension of physical reality rather as the independent area of different law principles. Finally, it can be noted that Napster case was a first and major litigation based on the ISPs civil liability ascription and all later similar litigations in one way or another referred to the findings of this case.

Another very important case is Tiffany (NJ), Inc. v. eBay, Inc.\(^{122}\) in which eBay\(^{123}\) was sued for secondary trademark infringement when it refused to extensively monitor its online auctions and removed only those items which can be proved with certainty being counterfeit. In this case court took a different approach (internal rather than external) than in Napster case and decided that eBay was not liable for the infringements made by third parties. Court indicated that eBay according to previously analyzed DMCA and CDA legislation was acting as a mere intermediary and thus was not liable for the violations committed by the actors it did not control\(^{124}\). eBay also obeyed notice and takedown rule and after sufficient proves were presented acted expeditiously to remove illegal goods from its auctions. Furthermore, court in this legislation adopted the rule of least cost enforcer. Under this rule, the party who can prevent infringement with the least costs is the one who must do it and if it does not conform it can be held liable for it. Rephrasing the court, it can be stated that “if Tiffany is a rational actor, willing to pay up to the amount that it would cost them to take its own enforcement actions, this suggests that eBay was not the least cost enforcer after all”\(^{125}\). The adoption of cost/benefit analysis in this case can be considered as a new phase of the ISPs civil liability litigation process because in the age of extensive Internet usage such analysis can be considered as one of the backgrounds of prescribing responsibility to ISPs.

Finally, the Perfect 10, Inc. v. Amazon.com, Inc., Google, Inc. and others\(^{126}\) case must be mentioned. In this case Perfect 10\(^{127}\) sued a number of third-party web site publishers (including Google as the major one) that placed images obtained from Perfect 10’s subscription-only area on their own websites, violating Perfect 10’s terms of service and copyright. Perfect 10 believed the linking to the images, caching and thumbnails constituted direct infringement of its intellectual property. According to the DMCA and

\(^{120}\)See supra note 112: F. A. PASQUALE, p. 192.

\(^{121}\)The notion of indirect financial benefit is very important in Napster type litigation processes. See id.


\(^{123}\)eBay is a company that manages eBay.com - an online auction and shopping website in which its users can buy and sell various goods and services worldwide.

\(^{124}\)See supra note 122: USA case: Tiffany (NJ), Inc. v. eBay, Inc.

\(^{125}\)See supra note 52: M. MACCARTHY, p. 26.

\(^{126}\)See USA case: Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007).

\(^{127}\)Perfect10.com was online photo gallery featuring high resolution photographs of women who have not had cosmetic surgery.
previous cases, the court stated that Google could be liable for contributory infringement if it: “(a) had knowledge that infringing images were available using its search engine; (b) could take simple measures to prevent further damage to the copyrighted articles; and, (c) failed to take such steps”\(^{128}\). Because Google passed this test and proved that it was simply making the web search faster and complex, the court found it not guilty for displaying links to copyright protected images. In reaching this result, “the court relied largely on the transformative nature of the thumbnails Google created, which, by facilitating the public’s ability to search the web for images, serve a different purpose than the original images, which are designed to entertain”\(^{129}\). This aspect of the decision is also very important because it showed that not only the legal approach to the civil liability of ISPs matters but also valuable public benefit which is acquired through new cyber technologies must be considered in deciding this type of cases.

In general, USA has a different approach to the ISPs civil liability than some EU countries. The biggest differences are the considerations in the decisions of courts of free speech policy, cost/benefit analysis and public value of technologies. It must be also noted that USA courts apply a more internal approach to this problem and usually treat ISPs with less scrutiny than other actors in similar situations.

In the next section of this part of the article the situation in this area in Lithuania will be presented and the main aspects of a relatively young law system related to cyber law and the ISPs civil liability will be analyzed.

### 3. LITHUANIAN APPROACH TO THE CIVIL LIABILITY OF ISPS

#### 3.1. MAIN ASPECTS OF THE “LAW ON ELECTRONIC COMMUNICATION” AND ADDITIONAL DECISION BY THE GOVERNMENT

Certain activities of the ISPs (including provision of Internet access to natural and legal entities and its technological implementation) and its liability in Lithuania are regulated by the “Law on Electronic Communication of the Republic of Lithuania”\(^{130}\) and by the Decision No. 290 by the Government of the Republic of Lithuania as of March 5, 2003\(^{131}\).

The mentioned law centers on regulation of technological implementation of ISPs services and it does not legislate the relationships among ISPs and other parties, including

---

\(^{128}\) See supra note 36: J. D. LIPTON, p. 112.


\(^{131}\) See: Regarding the approval of the control of information not to be published on public computer networks and the procedure of distributing restricted public information, Decision by the Government of the Republic of Lithuania (March 5, 2003, No. 290).
between all the content transmitted through its networks\textsuperscript{132}. Because no other laws regulate general or certain activities of ISPs in Lithuania, such a lack of legislation can be considered as a biggest drawback of the Lithuanian legal system in the area analyzed. Theoretically this lacuna of law can be filled by courts’ decisions but, having in mind presented hardships faced by the courts of other countries which have full legislation of the ISPs civil liability for the information transmitted, such recourse cannot be relied on.

The main legislative act by which civil liability to ISPs can be ascribed is the previously mentioned Decision by the Government of the Republic of Lithuania. As the restriction to distribute and/or publicly disclose information off-the-record (as defined by the “Law on Protection of Youths from Negative Public Information of the Republic of Lithuania”\textsuperscript{133}, the “Law on State Secrets and Official Secrets of the Republic of Lithuania”\textsuperscript{134} and other laws) in public computer networks is established in the mentioned decision\textsuperscript{135}, ISPs shall take all possible measures to restrict unlawful online activity. This decision also establishes that the approved by it procedures are applicable to the wide range of ISPs\textsuperscript{136}.

Several main aspects of this legal act can be pointed out. Firstly it can be noted that this decision adopts external approach to the ISPs civil liability therefore that it does not mention any safe harbor provisions for ISPs. On the one hand, it can seem that courts can use it in their own discretion and hold any ISPs liable for any illegal information transmitted through its network. On the other hand, it is obvious that such a broad application is impossible in today’s situation when Internet has become one of the main parts of social and economic life of the country and more clear regulation must be established. Secondly, because of such broad scope of its regulation (and also because of the provisions which are outdated and completely inapplicable in certain situation) this decision practically is not enforced at all because no governmental institution is able to cope with policing whole cyber space of Lithuania. While the direct application of the ECD without local legislative acts is impossible, situation in the area remains uncertain. It is clearly seen when analyzing jurisprudence of the courts in Lithuania where only few cases of civil liability of ISPs can be found.

\textsuperscript{132} The mentioned law relates exclusively to technological side of the intermediation process. See \textit{supra note} 130: Law on Electronic Communication, Art. 1 and 2.
\textsuperscript{133} See: Law on Protection of Youths from Negative Public Information of the Republic of Lithuania (September 10, 2002, No. IX-1067).
\textsuperscript{135} See \textit{supra note} 131: Decision by the Government, Art. 5.
\textsuperscript{136} It is stated that provisions of the procedure are “applied to legal subjects of the Republic of Lithuania, also legal subjects of foreign states, which, despite the fact that they do not live (are not established) in the Republic of Lithuania, yet they concentrate their entire activity (related to the distribution of public information in public computer networks) or its part within the territory of the Republic of Lithuania and use the services of a public communications network provider registered in the Republic of Lithuania and/or the services of information hosting providers operating in Lithuania, to distribute public information”. See \textit{id.}, Art. 3.
3.2. ANALYSIS OF THE MAIN CASES OF THE CIVIL LIABILITY OF ISPS IN LITHUANIA

Because of the lack of certain legislation of the ISPs civil liability, most of the cases in the area are based more on privacy protection, copyright enforcement and gambling regulation laws than on the Decision by the Government of the Republic of Lithuania.

One of the main cases of the ISPs civil liability is the recent ongoing case *Microsoft Lithuania v. Linkomanija.net*[^137^]. *Microsoft* sued owners of *Linkomanija.net*[^138^] site for copyright infringements made by it while offering to share torrents with links to illegal *Microsoft* production downloads. Despite that this case is not yet decided, several main aspects of this litigation can be pointed out. Firstly, this case, despite being a clear ISPs civil liability case, because of the mentioned lack of legislation is based on violations of copyright and intellectual property laws. Secondly, because of such legal background, plaintiff cannot use earlier presented theories or approaches to the ISPs civil liability and thus its legal arsenal is very weak. This weakness was proved in intervening decision of the Appellate Court of Lithuania which refused to grant injunction (suspension of all services related to torrent sharing) against *Linkomanija.net* site. The court mainly based its decision on the lack of prima facie prove that this site was involved on illegal activity[^139^]. Plaintiff could not collect enough facts to establish that *Linkomanija.net* was involved in illegal distribution of *Microsoft* production and one of the main reasons for this was an absence of procedure according to which civil liability to ISPs for content transmitted could be ascribed. Notwithstanding the final outcome of this litigation, it must be stated that current situation in Lithuania in the area concerned is not favorable for both ISPs (who cannot predict how certain cases will be decided) and for plaintiffs seeking to safeguard their interest (because of the unclear procedures of its implementation).

Another case that is still ongoing but its findings can have a significant impact on the development of the ISPs civil liability system in *Lithuania is Lithuanian Gambling Organizers Association v. Unibet, bwin, Triobet and others*[^140^]. In this case gamblers’ association sues various online gambling organizers and various Internet connection providers for providing access to online gambling sites, which do not have official licenses needed to engage in gambling activities in Lithuania. This case is still in its primary phase but first interim decisions by various courts can be already treated as trending direction in these types of cases. For example, in this case applicants filed a preventive action – they asked to prohibit the defendants to take certain actions (allowing to participate in online gambling activities without having required licenses) in the future and thus to prevent possible damages. Applicants stated that without applying the provisional protection

[^137^]: See Lithuania case: ongoing case *Microsoft Lithuania v. Linkomanija.net* in District Court of Vilnius.

[^138^]: *Linkomanija.net* is Lithuanian website offering its users possibility to download various content (most often copyrighted video, audio or software files) using specific “torrent” download system.

[^139^]: See Lithuania case: *Microsoft Lithuania v. Linkomanija.net*, Appellate Court of Lithuania (May 13, 2010; No. 2-652/2010).

[^140^]: See Lithuania case: ongoing case *Lithuanian Gambling Organizers Association v. Unibet, bwin, Triobet and others* in District Court of Vilnius.
measures the damage suffered by them would only increase and the enforcement of the final court decision (if it is in favor for applicants – that is the provision of online gambling services without certain licenses would be ruled unlawful) would become more difficult. In the view of such circumstances, the application of the applicants was satisfied and the provisional protection measures were applied: a ban on the defendants to take actions related to the provision of betting organization services, and advertising for persons located in the Republic of Lithuania, and the prohibition of all possible accesses via the public computer network operating in the Republic of Lithuania to the Internet portals bwin.com, triobet.com and others. The higher (appellate) court of Lithuania, to whom complaint for this decision by respondents was brought, withheld the primary decision by stating that ISPs that provide certain online gambling services as well as ISPs which provide possibility to access those Internet pages are the ones who have to take certain actions to suspend such services until the final decision whether the provision of online gambling services without acquiring license is lawful is made. This interim decision clearly shows that courts adapted external approach and did not analyze whether ISPs who merely provide Internet connection to general users can be ordered to factually filter all data stream in order to prohibit access to certain online gambling sites. Notwithstanding final decision in this case, these interim findings demonstrate that without a clear regulation in the area and lack of basic laws, courts are trying to fill this gap and can come up with decisions that can be hard to implement. They can also have a negative economic and social effect on Internet and its law development.

In the next part of the article possible conceptual background for creating a unified global ISPs civil liability regulation will be presented and its basic potential principles will be outlined.

III. CONCEPTUAL BACKGROUND FOR UNIFIED CIVIL LIABILITY REGIME OF ISPs

As it was shown in previous parts of this article, various legal systems enact different legal theories and approaches to the ISPs civil liability and therefore usually different results of similar type of litigations are possible. In order to better deal with the ISPs civil liability problem in global scope, three main liability regimes which could be used as a background for enacting further legislation mechanism can be pointed out. These are the following: 1) negligence (which encompasses notice-based liability), 2) strict liability, and 3) non-liability legal regimes. All of them correspond to different approaches to the ISPs liability, although it is obvious that for unified global approach to the ISPs civil liability problem certain mix of these regimes will most probably be used. In the next subsection of this article all these regimes are presented, their main aspects (including economic and social implications) are pointed; at the end, basic principles for conceptual model of global regime of the ISPs civil liability are introduced.

See Lithuania case: Lithuanian Gambling Organizers Association v. Unibet, bwin, Triobet and others, District Court of Vilnius (July 2, 2010; No. 2-6458-578/2010).

See Lithuania case: Lithuanian Gambling Organizers Association v. Unibet, bwin, Triobet and others, Appellate Court of Lithuania (December 30, 2010; No. 2-1585/2010).
1. NEGLIGENCE LEGAL REGIME OF THE CIVIL LIABILITY OF ISPS

„Imbedded in the … law as “distributor liability,” … regime [of negligence] turns on notice to the defendant, since knowledge of the allegedly injurious content gives rise to a duty on the part of the ISPs.”\(^{143}\) Negligence in this regime can be traditionally referred as a “conduct that fails to adhere to the legally prescribed standard for protecting others against an unreasonable risk of harm”\(^{144}\). As it was mentioned earlier this legal regime employs notice – based approach therefore it can be stated that it corresponds to passive-reactive (“ex-post”) approach that was presented in previous parts of the article.

Today this is the most popular regime in major jurisdictions around the world\(^{145}\) and it can be stated that it is a “global norm … to establish passive-reactive schemes that require or permit intervention in third-party communications upon receiving allegations of copyright infringement.”\(^{146}\) As it was pointed out previously in the article, according to this approach ISPs may be not held liable if it acts according to certain criteria and removes infringing information (data) after notice of its existence was presented to them. In consideration of this main aspect of the legal regime of negligence, primary functions of legal mechanisms based on it would be to establish rules according to which mentioned notice to ISPs for infringing content is provided, time and scope of ISPs reaction to this notice is defined, scope of civil liability if failing to act is incurred, etc.

Despite mentioned broad perception of this regime, several main drawbacks of it must be pointed out. Firstly, certain discrepancy exists between so called safe harbor provisions of ISPs if it reacts to notice and scope and intensity of this reaction. „Under the existing laws ... intermediaries must remain passive-reactive in order to obtain immunity from liability for copyright infringements occurring on their networks. The more active intermediaries are in the hosting or transmission process, the less likely they are to be protected by safe harbors.”\(^{147}\) This inconsistence is partly caused by the lack of clear rules according to which ISPs must exercise due care of the actions taken by third parties while using certain ISPs provided services. As it was mentioned earlier, establishment of the set of such rules is one of the main goals that must be achieved in order to implement legal regulation of the ISPs civil liability based on negligence legal regime. On the other hand, because of the all-embracing role of Internet it cannot be reached so easily.

Second drawback of this legal regime is its social-economic inefficiency. It is stated that “negligence regime creates a common-law sanctioned externality by permitting a certain level of expected costs to be imposed on the public. Therefore, imposing a negligence or distributor regime is economically inefficient”\(^{148}\). This can be also explained

\(^{143}\) See supra note 95: M. Schruers, p. 235.

\(^{144}\) See id., p. 233 – 234.

\(^{145}\) Such approach exists in the laws of Australia, Canada and China, the most of European Union (including France and Germany), Japan, New Zealand, Singapore, South Korea, the United Kingdom and the United States. See supra note 43: J. de Beer and Ch. D. Clemmer, p. 378.

\(^{146}\) See supra note 43: J. de Beer and Ch. D. Clemmer, p. 377.

\(^{147}\) See id., p. 405.

\(^{148}\) See supra note 95: M. Schruers, p. 240.
through the scope of usage of ISPs services. Because a negligence rule is not ascribing civil liability for those injuries that could not efficiently be prevented, the scope of ISPs service providing activity will not take into account the social cost of injuries incurred by some users. This happens because of the infringing content is being spread so broadly. Consequently, the market price of Internet access will not reflect the true social cost of the industry – it will be too low and ISPs will sell too many accounts to users who in turn will create too much possibly harmful third party content. 149

And finally third drawback of this legal regime is that when “[ISPs] ... remove[s] only as much content as it receives notice of, the ISPs forfeits any independent determination of how much content to remove.” 150 Consequently ISPs are becoming less interested in content regulation and all policing activity is left to certain governmental or private supervising authorities or even users themselves.

To conclude, because of the mentioned deficiency of negligence legal regime in some instances strict liability legal regime of the ISPs civil liability is enacted as a background for the regulation system of this issue.

2. STRICT LIABILITY LEGAL REGIME OF THE CIVIL LIABILITY OF ISPS

“In a strict liability regime, an injurer is liable to all victims regardless of the care with which he or she conducts activities, even if the exercise of due care would not have prevented the damage.” 151 It can be noted that this regime enacts previously mentioned “ex-ante” or active-preventative approach to the ISPs civil liability. As it was stated earlier in this article, “entertainment industries, government legislators, and regulatory agencies increasingly are pressuring online intermediaries to play a more active role in preventing copyright infringement ex-ante.” 152 It is obvious that this regime is mostly beneficial to parties interested in protecting their interests in cyber space (copyright holders, privacy activists, opposing parties of online gambling, etc.).

In order to implement this legal regime’s mechanism or structure of the scope of the ISPs civil liability, clear rules of online operation and supervision by enacting certain set of laws must be established. One example of this can be found in recent opinion of Advocate General of ECJ in which it was stated that “hosting providers can be deemed to have “actual knowledge” (or awareness) when there is an infringement of a trademark, and that infringement is likely to continue regarding the same or similar goods by the same user.” 153 Such interpretation of ECD could mean that in the future at least in the EU area some sort of strict liability regime can be introduced at least when referred to repeated or common infringements made by using certain services provided by various ISPs. As it was

149 See id.
150 See id., p. 245.
151 See id.
153 Notwithstanding that opinion of Advocate General of ECJ is not binding upon ECJ such trend shows that some changes in the legislation related to the civil liability of ISPs may be under way. See: P. VAN EECHE AND M. TRUYENS, “Advocate General Clarifies the Status of Hosting Providers under EU Law”, 14 NO. 8 J. Internet L. 29 (2011).
mentioned earlier, explicit rules to implement this regime should be created. As Advocate General also pointed out in his opinion “the crucial condition [in implementation of this regime] is that the hosting provider can know with certainty what is required from him, and that the injunction [of infringing actions] does not impose impossible, disproportionate, or illegal duties like a general obligation of monitoring”154.

Due to its stringent approach to the ISPs civil liability it is certain that this legal regime will not prevail in its pure form in the global perspective. Also, most probably it will be used as a part of some type of mixed approach. This proposition can be also grounded by analyzing the main drawbacks of this legal regime.

The first and main problem is “reductive effect of speech”. Because of the strict liability ISPs respond to any notice of infringing information (data) on their network and therefore immediately remove it rather than investigating and mitigating the liability scope with potential victim. Such ISPs actions, when content which does not actually infringe any law is removed because of mere danger of potential litigation costs, have implications on free speech spread on Internet. Socially and economically this effect can be explained as “there is merely “too much” Internet use ... [therefore] the corresponding “accident” costs (from alleged defamation, etc.) exceed the social benefits”155.

The second drawback of strict liability legal regime is that it undermines the “network effect” of the Internet. “A “network effect” … occurs when the utility that a user derives from consumption of the good increases with the number of other agents consuming the good.” 156 This effect also can be treated as one of the most important function of the Internet. If strict liability regime is introduced in full scope, some of the users would reduce their usage of certain ISPs services and this would affect other users. It can be stated that the efficiency of imposing strict liability would be negative because benefits achieved by it would be much smaller then losses incurred by global ISPs users’ community due to mentioned “network effect”.

It can be summarized that because of the problems mentioned above “imposing strict liability on ISPs would decrease the amount of Internet use without assuring a corresponding reduction in injuries”157 and therefore usage of pure strict liability regime is not acceptable and most probably only some principles of it will be used in development of the global and universal ISPs civil liability scheme.

3. NON-LIABILITY LEGAL REGIME OF THE CIVIL LIABILITY OF ISPS

Non-liability legal regime can be defined as a conditional immunity regime – „upon meeting the conditions of the law ISPs are afforded statutory immunity from suit”158. This regime can also be regarded as self-regulatory regime there ISPs can be held non-liable for

154 See id.
155 The socio-economic analysis of the influence that certain models of ISPs’ civil liability ascription have on the provision of intermediation services must be taken into consideration when analyzing possible legislative mechanisms in the field. See supra note 95: M. SCHRUERS, p. 249.
156 See id., p. 250.
157 See id., p. 253.
158 See id., p. 231.
the information transmitted by third parties when they engage in good faith monitoring. The application of this regime is a clear example of earlier mentioned external approach where ISPs can only be held liable for negligent actions performed directly and willfully by ISPs themselves. One of the best examples of application of this regime is the already discussed CDA\textsuperscript{159} in USA. Legal scholars point out several advantages of this regime.

First and most important point of non-liability civil regime is the principle of network neutrality\textsuperscript{160}. If we would apply negligence or strict liability legal regimes, some ISPs would have to engage in sorting content floating through them in order to avoid civil liability and thus would contravene principle of network neutrality.

Second advantage of this regime is that “[a] “competitive” or “open” communications policy sacrifices the order, predictability and stability of a planned policy for greater allowance of market entry and (backers believe) faster technological development”\textsuperscript{161}. This means that despite possibility to allow some parties of analyzed transactions to escape responsibility completely, non-liability legal regime institutes suitable environment in which social and economic development of both Internet and cyber law is most potential.

Thirdly, application of this regime minimizes economic inefficiency when ISPs, as least cost avoiders, engage in full-scale content monitoring and marginal costs of Internet usage rise unproportionally. It is stated that “just because ISPs are able to prevent subscriber misconduct cheaply does not mean that they should be burdened with the cost of preventing spread of [illegal content] and if unsuccessful, pay damages and have criminal liability imposed on them”\textsuperscript{162}.

Finally, the opinion of one of the biggest associations of ISPs in the world – The United States Internet Service Provider Association – can be mentioned as an authoritative source to assess practical implementation of the mechanism of civil liability ascription to ISPs. “As a general rule, liability for Internet content should rest with the creator or initiator of the illegal content and not with an entity that retransmits, hosts, stores, republishes, or receives such content.” \textsuperscript{163} It must be also noted that ISPs under non-liability regime should retain the right to block or filter traffic of data and to obtain immunity from liability for such action, if no direct negligent actions of ISPs are taking place.

On the other hand, as one of the main drawbacks of non-liability regime possible negative social effect can be mentioned. It occurs when ISPs, as least cost avoiders, do not take any certain actions to restrain access to illegal content. In such situations the end users or injured parties would have to play a more active role in preventing or stopping

\textsuperscript{159} See \textit{supra} note 113: CDA.


infringements. Such behaviour would be more costly and economically inefficient compared to actions which can be taken by ISPs.

Having presented three different legal regimes of the ISPs civil liability, it can be summarized that certain choice which will be made in near future will not include pure form of one of the regimes and most certainly would encompass mix of several regimes. Possible conceptual background for the mechanism of civil liability ascription to ISPs is presented in the last section of this part of the article.

4. POSSIBLE CONCEPTUAL BACKGROUND FOR THE UNIFIED ISPs’ CIVIL LIABILITY REGIME

As it was presented in previous sections of this article, there are several types of legal regimes on which background of possible global unified model of the ISPs civil liability ascription can be constructed. Such common background and its novel approach to the issue discussed is a mandatory part of future global Internet law. It is stated that “however, in the end, the impact of these issues on the future economic development in the online world is not to be underestimated [l]aw needs to keep up with the pace of changes in the online world that have become an important economic factor”\textsuperscript{164}. As it was shown in the article, currently the lack of legislation or clear rules of its implementation puts courts in primary positions in dealing with this problem. Because ISPs are an essential component of the normal functioning of the Internet and its various subsidiary services associated with it, courts have begun to develop the case law governing the ISPs civil liability for subscriber infringement along sensible lines. Unfortunately, there is no guarantee that those results will be followed in the future\textsuperscript{165}. It can be also mentioned that “from the [ISPs] point of view, a clear and harmonized approach is needed more than a victory in one country’s courtroom”\textsuperscript{166}.

Having made extensive analysis of theoretical base for the ISPs civil liability and having examined practical legal regimes in the area, it can be proposed that most probable outcome in the near future will be the usage of mixed (negligence, strict and non-liability) legal regime to ascribe responsibility for third parties actions. Several main aspects (principles) of such new regime which will most likely be applied in its establishing can be pointed out.

Firstly, principle of Internet freedom will have to prevail in order to secure highest efficiency of Internet communication. “The freedom of Internet communication, which is firmly rooted in international human rights law, is at the core of Internet freedom.”\textsuperscript{167} Since one of the main problems today is unclear function of ISPs in establishing illegality of the content, “the administrative authority should be the only party competent to order the removal (take-down measures) of “manifestly illegal” content to prevent the continuation of

\textsuperscript{167} See id.
the alleged infringement". As long as the content is only “allegedly” illegal, there should be no obligation for the host provider to act expeditiously to remove the content since the illegal nature of the content has not been established. It is also very important that above mentioned principle would prevail over various theories and approaches used today by courts. In order to achieve this, clear legislation with adequate notions must be enacted.

Secondly, privacy aspect is very important in sustainable development of the future ISPs civil liability system. This aspect in certain ways can be contrary to the principle of Internet freedom, thus “whereas freedom of expression may be restricted in favor of the rights of others and in particular the right to privacy, any restriction must be proportionate to the aim pursued...states have to strike a fair balance between privacy on the one hand and Internet freedom on the other hand”. It can be assumed that only clear and unambiguous treatment of Internet privacy in legislation can lead to unimpeded functioning of cyber space as a whole.

Thirdly, internal or technology-friendly approach should be in the center of the ISPs civil liability ascertainment. “Technologies and business methods that have been widely adopted [can] ... no longer be treated as suspect simply because they can be used for infringement.” As it was argued before, internal approach to ISPs services and products can be helpful in obtaining equitable solutions in the area discussed. It must be also mentioned that enacting Internet filtering technologies is undesirable and “they should only be used as a last resort, in cases where the removal of online content is impossible”. This notion is very important because even if internal or technology-friendly approach is adopted by legislation and courts, usage of various Internet filters can lead to violations of formerly mentioned Internet freedom and privacy principles.

Fourthly, new principles of territorial jurisdiction of the ISPs civil liability must be established. On one hand, “the effects doctrine giving jurisdiction over foreign acts provided that they produce effects within the own territory must be adapted to the ubiquitous nature of the Internet [must be enacted and on the other hand] jurisdiction [must] expand to a state's country code Top Level Domain which becomes cyber territory” in order to facilitate definite procedural mechanism of this type of legislation.

Finally, ISPs differences must be regarded as one of the main factors while deciding on various cases of the civil liability for transmitted information by third parties. As it was mentioned before, there are many different types of ISPs (from basic Internet service providers to complex websites operators) and each of them must be treated correspondingly

---

168 Such administrative authority must not only have relative competence but also certain clear and comprehensive set of rules must be created in order to achieve desired level of sustainable regulation. See: J. ZIMMERMANN, P. AIGRAIN and others, Legal Liability of Internet Service Providers and the Protection of Freedom of Expression Online (2010); <www.laquadrature.net/files/LQDN-20101105-Response_e-Commerce.pdf> [visited April 07, 2011], p. 4.

169 See id., p. 6.

170 See supra note 166: J. ZIMMERMANN, P. AIGRAIN and others, p. 6.


172 See supra note 168: J. ZIMMERMANN, P. AIGRAIN and others, p. 12.

173 See id.
and adequately in the way they operate and technology they use. This is important in order to justly ascribe legal responsibility. “A clear understanding of the pulse of new technology innovation necessitates the incorporation of existing assessment framework to prevent unwarranted inferences and “chilling affects” to the detriment of the [users] and public as a whole.”

In summary, it can be stated that only versatile incorporation of Internet freedom and online privacy, cyber-territorial and other principles can guarantee not only sustainable and sound development of the global unified ISPs civil liability system but must also be treated as one of the cornerstones of the whole still evolving Internet law.

**CONCLUSIONS AND PROPOSALS**

Based on the analysis of theoretical background of the ISPs civil liability, examination of the main cases in this area around the world, as well as having presented the main legal regimes based on which global system of liability ascription to ISPs for third parties’ actions can be constructed, the following conclusions are drawn and proposals are suggested:

1. Theoretical background of the ISPs civil liability is an important part of the new emerging Internet (cyber) law. Furthermore, its analysis can contribute not only to the better understanding of underlying processes of legal interaction between main actors in cyberspace but also helps to construct an analytic framework that would be useful in determining the appropriate scope and under what circumstances and rationale legal responsibility can be ascribed to the ISPs for the actions of third parties.

2. According to the basic notions of constitutive and “speech-act” theories, ISPs can be held liable for their users’ behavior when the former commit infringement providing basic Internet services to an infringing user. This ascription of liability is possible because of the mere nature of ISPs who automatically and routinely reproduce and distribute protected material in response to users’ requests.

3. Under the doctrine of “respondeat superior” strict liability can be imposed on abnormally dangerous activities (among which almost all services of ISPs can be placed) because the risk of harm is great and cannot be eliminated by the exercise of due care.

4. Secondary liability – contributory (with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another) and vicarious (the right and ability to control a third party’s infringing activities and receives of a direct financial benefit from the infringement) – theories are the main used today in courts all over the world to base legal responsibility of ISPs for third parties’ actions.

5. Different approaches (“ex-ante” and “ex-post”, external and internal, exceptionalists and non-exceptionalists, etc.) to civil liability of the ISPs are influencing judicial reasoning and outcomes in related cases in various jurisdictions. Therefore, the lack of one prevailing approach can be regarded as the biggest threat to sustainable development of international Internet law.

6. Theoretically ascription of legal responsibility to the ISPs for third parties’ actions can be shown as a system of opposing direction of civil liability and regulation processes where regulation and civil liability streams are directed through ISPs accordingly towards end users and initiators of infringements.

7. “The European Community’s Electronic Commerce Directive” (ECD) is one of the main legal acts among other things regulating civil liability of the ISPs. Its basic principles are the following: 1) establishment of a horizontal exemption from liability for ISPs when they play only a technical role in transmitting third party information, 2) guarantee of circulation of information services throughout the European Community in full compliment with freedom of expression and 3) no general obligation for ISPs to engage in monitoring activity.

8. Different EU member states interpret provisions of the ECD differently. Such divergent approach determines not only that ISPs are having difficulties in adapting to diverse legal treatment of civil liability, but also that courts, who are trying to fill this gap in law system with their decisions, are failing to go along with a pace of Internet technology innovations. Such situation reveals an evident lack of unified legislative position in the area discussed.

9. Main legislative acts in USA regarding the ISPs civil liability are – “Digital Millennium Copyright Act” and “Communications Decency Act”. Their biggest difference compared to EU’s ECD is much broader and more detailed provisions for ISPs “safe harbors” (various rules of exceptions from civil liability) and more complex analysis for requests of injunction against ISPs or their users.

10. A distinct approach to the ISPs civil liability from analyzed EU countries’ jurisprudence can be found in US legislation. Among its biggest differences are considerations in the decisions of courts of free speech policy, cost/benefit analysis and public value of technologies. It must be also noted that US courts apply a more internal (exceptionalistic) approach to this problem and usually in similar situations treat ISPs with less scrutiny then courts in other mentioned countries.

11. There is no law which directly deals with the ISPs civil liability in Lithuania. Furthermore, the main legislative act is an outdated decision by the Government concerning the control of information. The direct application of the ECD without local legislative acts is impossible and this lack of legislation can be considered as the main problem of responsibility ascription system. That is because due to complex nature of various legal cyber-relations, courts are not able to fill this lacuna of law with their decisions.

12. Only few examples of the ISPs civil liability can be found in case law of Lithuania. Their analysis shows that without clear regulation in the area, courts come up with the decisions that are hard to implement and also have negative economic and social effect. This situation is as well becoming an obstacle to the development of the Internet law and Internet as technology itself, therefore a clear and complex system of concerned laws is a must in a near future.

13. Negligence (notice based) legal regime of the ISPs civil liability is the most popular regime used today. It could become an important part of a possible new global unified system of responsibility ascription, if its main drawbacks – lack of the clear rules of engagement and social-economic inefficiency – are eliminated.
14. Strict and non-liability legal regimes because of their marginal approaches to the problem – from active-preventative (“ex-ante”) to completely voluntary (“the Good Samaritan”) – will more likely not be used as a background for possible legal regulation of the ISPs responsibility. Rather they could become supplementary tools while dealing with the issue discussed in certain legal situations.

15. Versatile incorporation of Internet freedom, online privacy, internal (technology-friendly) approach, cyber-territorial jurisdiction, consideration of different functioning of various Internet service providers and other principles and their corresponding alignment with the mix of the mentioned legal regimes is probably the best possible solution to sustainable and sound development of the global unified ISPs civil liability system.

Due to the scope and volume of this article, topics and problems of complex ascription of civil liability for third parties’ action to different types of ISPs, the influence and overall relation with public and private international law as well as certain legislative procedures were not encompassed and can be regarded as the new dimensions for expanding this research in the area discussed in the future.

**LITERATURE**

**BOOKS**


**JOURNALS**


YEN, A. C. *Sony, Tort Doctrines, and the Puzzle of Peer-to-Peer.* Boston College Law School Faculty Papers, No. 31 (2005), p. 11, 40.

**LEGAL DOCUMENTS**


Regarding the approval of the control of information not to be published on public computer networks and the procedure of distributing restricted public information, Decision by the Government of the Republic of Lithuania (March 5, 2003, No. 290).

Digital Economy Act of UK 2010 (c. 24, April 8, 2010).

Belgium case: SABAM v. S.A. Tiscali (Scarlet). Tribunal de Première Instance de Bruxelles (June 29, 2007 No. 04/8975/A).


USA case: *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d1159, 1161 (2d Cir. 1971).
USA case: *In re: Aimster Copyright Litigation*, 334 F.3d 643, 654 (7th Cir. 2003).
USA case: *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007).
Lithuania case: *Microsoft Lithuania v. Linkomanija.net*. Appellate Court of Lithuania (May 13, 2010; No. 2-652/2010).
Lithuania case: *Lithuanian Gambling Organizers Association v. Unibet, bwin, Triobet and others*. District Court of Vilnius (July 2, 2010; No. 2-6458-578/2010).
Lithuania case: *Lithuanian Gambling Organizers Association v. Unibet, bwin, Triobet and others*. Appellate Court of Lithuania (December 30, 2010; No. 2-1585/2010).
Sweden case: Appellate Court of Sweden (November 26, 2010; No. B 4041-09).

**SANTRAUKA**

INTERNETO PASLAUGŲ TIEKĖJŲ CIVILINĖ ATSAKOMYBĖ UŽ TREČIŲJŲ ASMENŲ PERDUOTĄ INFORMACIJĄ; TEISINIO REGLAMENTAVIMO PROBLEMOS IR PERSPEKTYVOS

*Spartus interneto augimas ir skverbimas į visas socialinio ir ekonominio gyvenimo sritis yra susijęs su interneto paslaugų tiekėjais (IPT), suteikiančiais prieigos prie duomenų per viešo naudojimo kompiuterių tinklą ar juo prieigos paslaugas. Suteikdami šias paslaugas IPT kiekvienam vartotojui tuo pačiu leidžia naudotis neribota žodžio ir išraiškos laisve, tuo prisidėdami prie liberalios ir demokratinės visuomenės plėtros. Tuo pačiu IPT netiesiogiai daro įtaką ir neteisėtų informacijos platinimui internetu. Jos kontrolė, esant dideliais duomenų srautais, yra praktiškai neįmanoma. Vieningo teisinio reglamentavimo (tiek įstatymų, tiek ir teismų praktikos) šioje srityje nebuvinamas nulemia kovos su internetiniais nusikaitimais, tokiais kaip autorių teisių ar privatumo pažeidimai, azartiniai lošimai, vaikų pornografijos platinimas internete ir pan., problemas. Tai apriboja IPT galimybes apsiginti nuo trečiųjų asmenų civilinės teisės, susijusių su mėnesų nusikaltimų sukelta materialine ir nematerialine žala. Toks teisinis neapibrėžtumas netolimoje ateityje gali tapti ir interneto paslaugų plėtros stabdžiu, todėl vieningas interneto tarpininkų civilinės atsakomybės mechanizmo pagrindas.*

Šio straipsnio tikslas yra įvertinti IPT civilinės atsakomybės už trečiųjų asmenų perduotą informaciją nustatymo būtinių ir galimų jos apimtį, taip pat pristatyti pagrindinius principus, remiantis kuriuose buvusi galimas bendras globalus interneto tarpininkų civilinės atsakomybės mechanizmo pagrindas.
Siekiant įgyvendinti šį tikslą, straipsnyje yra analizuojamos pagrindinės IPT civilinės atsakomybės teorijos ir hipotetiniai atsakomybės priskyrimo metodai, aptariami pagrindiniai šios srities ES, JAV ir Lietuvos teisės aktai bei svarbiausios išnauginėtos ar nagrinėjamos bylos. Paskutinėje straipsnio dalyje pristatomi esminiai teisiniai režimai ir principai, remiantis kuriais būtų kuriama vieninga IPT civilinės atsakomybės sistema.

Įgyvendinus straipsnio pradžioje užsibrėžtą tikslą ir iškeltus uždavinius, pabaigoje prieinama prie išvados, kad tik įvairių teisinių režimų (pilnos, įspėjamosios ir laisvos atsakomybės) ir principų (interneto laisvės ir privatumo, kibernetinės jurisdikcijos ir kt.) suderinimas gali užtikrinti tinkamą ir darnią interneto teisės nagrinėjamojo srityje raidą.

PAGRINDINĖS SĄVOKOS

Internetas, interneto teisė, interneto paslaugų tiekėjai, civilinė atsakomybė.