NOTICE AND TAKE DOWN, ON CERTAIN ASPECTS OF LIABILITY OF ONLINE INTERMEDIARIES

“Notice and Take Down”, o některých aspektech odpovědnosti poskytovatelů služeb

Final Thesis

Author: Tomáš Elbert
Supervisor: Doc. JUDr. Michaela Zulkínová, CSc.
Date: 04. 01. 2011
DECLARATION

I hereby declare that I have written the final thesis alone, I have duly referred all the sources and literature that I have used within, and the final thesis was not used for the award of any other academic degree or diploma.

Prague ........................ Signature ..........................
Contents

Table of Abbreviations ............................................................................................................4
Abstract ......................................................................................................................................5

1. INTRODUCTION .................................................................................................................6
   1.1. Liability of online intermediaries ..................................................................................6
   1.2. ECD safe harbours and its transposition ........................................................................9
   1.3. Notice and Take Down ..................................................................................................14
   1.4. Thesis questions ..........................................................................................................15
   1.5. Method ........................................................................................................................16
   1.6. Assumptions ...............................................................................................................17

2. SCOPE .................................................................................................................................17
   2.1. Information society service provider ("ISSP") .............................................................18
   2.2. Hosting ........................................................................................................................22
   2.3. Object (content) ...........................................................................................................24

3. THE NOTICE ........................................................................................................................26
   3.1. Who may serve the notice .............................................................................................26
   3.2. Form of the notice ........................................................................................................28
   3.3. Necessary information ..................................................................................................29
   3.4. Truthfulness of the notice ............................................................................................32

4. DUTY TO ACT EXPEDITIOUSLY ......................................................................................33

5. REAPPEARING ILLEGAL CONTENT .................................................................................34

6. SHIFT TOWARDS MONITORING ......................................................................................37
   6.1. Volume of content ........................................................................................................37
   6.2. User-generated content as a source of income .............................................................38
   6.3. Online intermediaries are no longer endangered species ...........................................39
   6.4. Development in technology ........................................................................................39

7. CONCLUSION .....................................................................................................................40

Bibliography ..............................................................................................................................43
Table of Legal Instruments ........................................................................................................46
Table of Cases ............................................................................................................................47
Table of Documents ..................................................................................................................48
Czech Abstract ..........................................................................................................................49
Czech Summary ........................................................................................................................50
### Table of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTA</td>
<td>Anti-Counterfeiting Trade Agreement</td>
</tr>
<tr>
<td>2004 Act on ISS</td>
<td>Zákon č. 480/2004 Sb., o některých sluţbách informační společnosti a o změně některých zákonů [Act No. 480/2004 Coll., on certain information society services and on amendments to certain acts]</td>
</tr>
<tr>
<td>CDA</td>
<td>Communications Decency Act of 1996</td>
</tr>
<tr>
<td>DMCA</td>
<td>Digital Millennium Copyright Act 1998</td>
</tr>
<tr>
<td>ISS</td>
<td>Information Society Service</td>
</tr>
<tr>
<td>ISSP</td>
<td>Information Society Service Provider</td>
</tr>
<tr>
<td>NTD</td>
<td>Notice and Take Down</td>
</tr>
<tr>
<td>UGC</td>
<td>User-generated content</td>
</tr>
</tbody>
</table>
Abstract

The final thesis addresses certain aspects of current topic of online intermediaries’ liability for user-generated content (“UGC”). Under Act No. 480/2004 Coll., on certain information society services (“2004 Act on ISS”), which transposes e-Commerce Directive 2000/31/EC, online intermediaries in the Czech Republic benefit from “safe harbours”. Essentially, it means that online intermediaries can be held liable for UGC only if they had actual or constructive knowledge of illegality of the content.

This rule implicitly creates the so called “Notice and Take Down” procedure (“NTD`). Online intermediary upon receiving a notice, and thereby learning about the illegality of the content, is obliged to expeditiously take down the illegal content in order to preserve his immunity. However, NTD is neither expressly regulated within the ECD nor within the 2004 Act on ISS. Therefore, the purpose of the thesis is to illuminate NTD procedure and provide guidelines for it successful application within the Czech Republic. The thesis should be helpful not only to online intermediaries, but also to aggrieved parties serving notices. For this purpose the thesis looks not only at the ECD and its transpositions in various Member States, but also at American Digital Millennium Copyright Act 1998 that has been the main inspiration for the ECD.

First, the thesis outlines the scope of the 2004 Act on ISS. Then it explains that, although notices can be served anonymously and under certain circumstances with minimum information, it is not in the interest of notifiers. Notices with insufficient information may not cause actual knowledge on part of the online intermediary and therefore may be ineffective. The thesis also explains that online intermediary’s duty to act expeditiously will depend on both, the quality of the online intermediary and also the quality of the notified content. Expect that, online intermediaries need to be aware that although they have taken down certain content, their liability may be established if that content appears again and it is not automatically removed. The final chapter puts NTD into broader context and explains that NTD will need to be supported by other proactive measures on part of online intermediaries.
1. INTRODUCTION

1.1. Liability of online intermediaries

Mass media have marked year 2009 as internet’s 40th anniversary. However, from 1969, when Arpanet network was born, it took another twenty long years before World Wide Web system, the cornerstone of the internet as we know it, was developed. Having in mind this rapid recent development, it is understandable that some internet experts even in the middle of 90th still believed that Cyberspace, which was created by the internet, could function without any statutory regulation whatsoever.1 At the same time, other internet experts called for completely new system of legal rules in order to regulate activities on the internet.2 Both of these claims appeared to be unfounded. Instead, cyberspace has become part of our “real world”3 and online activity is therefore regulated by the national laws of the “real world”.

Nevertheless, there are also several specific legal rules and connected topics that are relevant only to online activities. These constitute the subject of internet law.4 The final thesis will address one of the most discussed topics of internet law, the objective liability of online intermediaries5 for content that is uploaded by third parties, the so called user-generated content (“UGC”).6

The internet is a telecommunication medium and therefore its essence is information, or in the words of the e-Commerce Directive (“ECD”),7 the content. Having in mind that the internet has become part of our daily world, it comes natural that even the communication of online content may be an illegal activity. For example content may be in breach of copyright, defamatory, infringing trademark protection, in breach of confidence,8 in contempt of court,9 or even in violation of criminal law (obscenity or indecency, child and extreme pornography, inciting racial hatred etc.).

---

1 e.g. famous cyber-libertarian John Perry Barlow, who published influential Declaration of the Independence of Cyberspace, (February 8, 1996 Davos, Switzerland)
3 For the most recent development of this trend see discussions on the concept of “Internet of Things”.
4 Internet law blends with other legal disciplines, such as computer law, ICT law or cyber law.
5 Also known as “ISPs” (Internet Service Providers), “ISSPs” (Information Society Service Providers) or just shortly “service providers” as in the DMCA and the ECD.
8 see Sir Elton John and others vs. Countess Joulebine and others (2001) QBD
Content provider, a person who uploads content, is obviously liable for such content in the same way as he would be for the similar activity in the “real world”. However, the question is whether online intermediaries whose services were used for communication of illegal UGC can be held liable for it? Whether certain level of objective liability may be imposed upon online intermediaries? It is not surprising that such question appeared in front of the court in the USA already in 1991. However, due to its complexity and also due to the recent evolution of the internet, this question was still not resolved satisfactorily.

The evolution that aggravated the question on liability of online intermediaries is called Web 2.0. The phenomenon called Web 2.0 represents the idea of collaboration of internet users. The cornerstone of the collaboration is UGC. Accordingly, online intermediaries serve as mere platforms for UGC in Web 2.0 environment. Indeed, many of these service providers usually do not produce their content at all. Their main purpose is to host and spread UGC. This trend goes so far that such service providers can be perceived as mere programs for connecting individual internet users rather than as content providers. We are talking about websites for sharing texts, videos and pictures (e.g. www.blogger.com, www.youtube.com, www.flickr.com), wikis for collaborative work (e.g. www.wikipedia.org), social networking sites (e.g. www.facebook.com, www.twitter.com), virtual worlds (e.g. http://secondlife.com, www.worldofwarcraft.com) and thousands of other websites providing manifold alternative services. To fully appreciate the context of the final thesis, Chapter 6 explains how further development of Web 2.0 influenced the liability of online intermediaries.

Before proceeding further, it must be also explained here, why aggrieved parties try to sue online intermediaries instead of the content providers. The reason for that lies in several salient features of the internet. First of all, providers of unlawful content usually stay in anonymity, or use merely nicknames to identify themselves in Cyberspace. Accordingly, it is often very easy for them to protect their anonymity and thereby difficult or even impossible for aggrieved party to sue them. Secondly, even if they are identified, they may be situated literally anywhere in the world. Consequently,

---

12 Identification based on unique IP address is often insufficient. First of all, IP addresses are usually dynamic, which means that different IP addresses are assigned every time computer is connected to the Internet. Secondly, it is not difficult for technical savvy offenders to mask their IP address (e.g. connecting through Virtual Private Networks (VPNs)). Last, but not least, you need to prove who was actually using the particular computer at particular moment.
it may be very costly and uncertain to sue them. Thirdly, it is often the case that providers of unlawful content are private individuals without sufficient wealth. Therefore it would not be reasonable to sue these content providers, if they are unlikely to pay up potentially awarded damages. Contrary to that, online intermediaries are usually not anonymous, they may be seated and therefore also sued in the particular state and most importantly in private disputes they may have sufficiently “deep pockets”. Moreover, the claimant may seek to prevent appearance of illegal content that is coming from more than one content provider and therefore it will be more effective to target online intermediary instead of suing every individual content provider.\textsuperscript{13} Notwithstanding the fact, that it might also be a strategy of the claimant to sue one online intermediary in order to motivate other online intermediaries to undertake proactive steps in preventing particular illegal content.\textsuperscript{14} Bearing these factors in mind, it is not surprising that online intermediaries are often held liable instead of individual users who are the original source of illegal UGC.

Naturally, online intermediaries were not willing to accept liability for UGC and argued that one should not “shoot the messenger”. This understanding of role of online intermediaries is more than appropriate in relation to online intermediaries in a narrow sense, such as mere conduit online intermediaries. These include access providers and online intermediaries providing the telecommunication networks that merely carry the content (e.g. AOL, BT Group, UPC Broadband or Tiscali). Their services are therefore very similar to the provision of telephone or even postal services. These access providers do not usually have any knowledge about the content of transmitted information and even less whether the content is illegal or not. Consequently, they are seen as mere messengers and therefore the common conclusion reached by the courts was that those online intermediaries were not liable for illegal UGC. Most influential European case reaching this conclusion was undoubtedly German CompuServe case, where managing director of access providing company was first held liable for distribution of child pornography, and later acquitted on appeal.\textsuperscript{15}

However, also other online intermediaries in a broader sense, as for example owners of web-sites that hosted UGC have enjoyed the same level of immunity as far as they did not have knowledge of illegality of content, did not edit such content and most importantly did not encourage sharing of illegal content. It was generally recognised that online intermediaries, as far as they had no prior or constructive

\textsuperscript{13} Angel, J and Reed, C, (eds), Computer Law: The Law and Regulation of Information Technology (6 end OUP, Oxford 2007) 240
\textsuperscript{14} Angel, J and Reed, C, (eds), Computer Law: The Law and Regulation of Information Technology (6 end OUP, Oxford 2007) 241
\textsuperscript{15} LG München I, 17.11.1999 - 20 Ns 465 Js 173158/95, or most recently for example Australian Roadshow Films Pty Ltd & Ors v iiNet Ltd [2010] FCA 24
knowledge of illegality of content, could not be held liable. Using Marsden’s words, online intermediaries were like three wise monkeys who hear no evil, see no evil and speak no evil.\textsuperscript{16}

Nevertheless, due to various types of online illegality, different laws in different states, and also different facts of particular cases, the level of immunity was far from clear. Consequently, online intermediaries have always been exposed to significant level of uncertainty in respect of their liability for UGC. In 2004, Reed has written: “There is growing international consensus that the way to solve this problem, particularly in respect of third party content [UGC] liability, is by granting intermediaries some immunity from liability”.\textsuperscript{17} He has continued that it is necessary to define the circumstances and limitations of this immunity. The ECD was an attempt in precisely that direction. The ECD set the level of immunity horizontally, notwithstanding whether copyright, defamatory or other legal rules were infringed. The thesis does not scrutinize the liability of online intermediaries, but instead its limitations. Moreover, it is focused only on the so called “Notice and Take Down” procedure, which inevitably arises from these limitations as described in Part 1.3.

\subsection*{1.2. ECD safe harbours and its transposition}

The e-Commerce Directive calls online intermediaries as \textit{service providers}, which the ECD defines information society service provider (“\textit{ISSP}”).\textsuperscript{18} This definition is explained in Part 2.1.

As it was pointed out, the ECD codified in that time already dominant opinion, that ISSPs shall not be held liable for UGC, unless they had actual or constructive knowledge about the illegality of user-generated content (“\textit{UGC}”). ISSPs are not to be held liable for UGC when providing these three services: \textit{mere conduit}, \textit{hosting} and \textit{caching}.\textsuperscript{19} These three activities, which will be now described in more detail, constitute for ISSPs the so called "safe harbours". They have in common ISSP’s lack of control over the content.

\textsuperscript{17} Reed, C, \textit{Internet Law} (2\textsuperscript{nd} edn CUP, Cambridge 2004), 122
\textsuperscript{18} The final thesis uses denomination “ISSP” in respect of online intermediaries to indicate legal regimes of the ECD and of its national transpositions. Otherwise, neutral term “online intermediaries” is used.
\textsuperscript{19} Categories in the DMCA are (a) Transitory digital network communications, (b) System caching, (c) Information residing on systems or networks at direction of users, (d) Information location tools.
It must be bear in mind, that it is wholly upon national legal order to regulate the liability of online intermediaries for UGC. The ECD merely limits such liability. Articles 12 to 14 ECD only stipulate that Member States shall ensure that the service provider is not liable, unless they had the knowledge of the content’s illegality etc. However, the ECD does not provide for consequences, when an ISSP breaches NTD regime or otherwise leaves the safe harbours of immunity.

First, Article 12 (1) ECD provides that ISSP acting as a mere conduit is not liable for UGC. According to Article 12 (1) ECD this means that the ISSP merely transmits the information or provides access to a communication network. It means that this article covers telecommunication companies and access providers as they were mentioned above (online intermediaries in narrow sense). Article 12 (2) ECD than explains that these activities:

"include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission."

Although Article 12 (2) ECD uses word “include”, which is not exclusive, it appears that actually only the activities fulfilling requirements of Article 12 (2) ECD qualify for mere conduit safe harbour for transmission or provision of access in the sense Article 12 (1) ECD. Mere conduit liability exemption therefore protects ISSPs that are truly sheer messengers, such as access providers or other operators of the telecommunication networks, which do not have any control over the content that they communicate.21

The safe harbour applies on condition that ISSP:

(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.

Secondly, Article 13 (1) ECD provides immunity where ISSP performs caching22 of the content. Article 13 (1) ECD describes caching as:

---

21 It was also suggested, and it indeed seems reasonable, that this group includes providers of instant messaging and voice over IP services. Polčák, P, ‘Odpovědnost poskytovatelů sluţeb informační společnosti’ (2009) 23 Právní rozhledy 837
22 (Web) Caching describes a practice where content is automatically stored on proxy servers, which are closer to the user and thereby enable faster access to the demanded information. For more information see Huston, G, ‘Web Caching’ <http://www.cisco.com/web/about/ac123/ac147/ac174/ac199/about_cisco_ipj_archive_article09186a00800c8903.html> accessed 04 March 2010
“the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request”

This definition must be closely followed. Arguably, there are certain types of caching services that do not satisfy this definition and therefore do not benefit from the safe harbour. These are, the so called “long term caching” and “mirror caching”, which do not benefit from the ECD protection since they are neither automatic nor intermediate.23

Protection in Article 13 (1) ECD applies on condition that:
(a) the provider does not modify the information;
(b) the provider complies with conditions on access to the information;
(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Thirdly, and for the purposes of the final thesis most importantly, Article 14 (1) ECD provides immunity to ISSPs hosting the content. For analysis what activities exactly fall within the category of hosting, please refer to Part 2.2. Immunity in Article 14 (1) ECD applies on condition that:
(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

To sum up, to keep these immunities, it is essential that an ISSP does not exercise any control over the content and therefore has no knowledge of the illegality. Especially the ISSP does not initiate the transmission, does not modify the content and does not exercise any control over the recipient of the service24 (the content provider). As Recital 42 ECD explains, the ISSP’s activity needs to be of mere technical, automatic and passive nature in order to benefit from these immunities. Moreover, to secure that these provisions are not circumvented on national level, the ECD stipulates in Article 15 that Member States shall not impose a general obligation on ISSPs to

24 Article (2) (d) ECD defines recipient of the service as “any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible”. This broad definition clearly covers anybody using the internet.
monitor the information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity.

The ECD was implemented in the Czech Republic by Act No. 480/2004 Coll., on certain information society services and on amendments to certain acts25 (“2004 Act on ISS”) on 29 July 2004.26 The act came into force on 7 September 2004, the very same day as it was declared. Author’s translation of the wording of the relevant provisions of the 2004 Act on ISS is following:

**Liability of intermediary service providers** [ISSPs]

§ 3

**Liability of service provider for content of transmitted information**

(1) The provider of a service, which consists of the transmission in a communication network of information provided by a user, or the provision of access to a communication network for the purpose of transmission of information, is liable for the content of transmitted information, only if he:

a) initiates the transmission,

b) selects the receiver of the transmitted information, or

c) selects or modifies the transmitted information.

(2) The acts of transmission and of provision of access referred to in paragraph 1 include also the automatic, short-term and transient storage of the transmitted information.

§ 4

**Liability of service provider for content of automatic, intermediate and temporary storage of information**

The provider of a service, which consists of the transmission of information provided by a user, is liable for the content of automatic, intermediate and temporary stored information, only if he:

a) modifies the information;

b) does not comply with conditions on access to the information;

c) does not comply with rules regarding the updating of the information, which are widely recognised and used by the relevant industry;

d) does interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

e) the provider does not act expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court has ordered such removal or disablement.

§ 5

**Liability of service provider for storage of content provided by a user**

---

25 Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů

26 According to Article 22 (1) of the e-Commerce Directive, the Directive ought to be implemented by Member States till 17 January 2002. However, the delay in implementation was not exceptional in respect of the implementation of any other directive.
(1) The provider of a service, which consists of the storage of information provided by a user, is liable for the content of information stored at the request of a user, only if he:

a) with regard to the nature of his activity and circumstances and nature of the case, could have known that the content of stored information or activity of the user are illegal, or

b) verifiably learned about illegal nature of content of the stored information or about illegal activity of the user, and he did not expeditiously take all the steps, which can be demanded from him, to remove or disable such information.

(2) The service provider referred in paragraph 1 is always liable for the content of stored information, if he exercises directly or indirectly decisive influence upon activity of the user.

§ 6

Service providers referred in § 3 to 5 do not have to

a) inspect the content of information that they transmit or store,

b) actively seek facts or circumstances indicating the illegal content of information.

The 2004 Act on ISS reverses the wording of the ECD, which states that ISSPs are not liable if. Contrary to that, the 2004 Act on ISS provides that ISSPs are liable only if. Moreover, the Explanatory memorandum to the 2004 Bill on ISS leaves no doubts that this wording was intentional and that the 2004 Act on ISS not only limits the liability of ISSPs, but also establishes it. From perspective of the Czech legal system this is very significant. Previously construction of ISSPs’ liability was very uncertain, because it would have to be established on vague provisions, such as general duty of prevention of threatening damages under § 415 of the Civil Code. Or in respect of criminal liability it would have to be established on even more uncertain construction of guarantee and interference doctrine (§ 112 of the Criminal Code). After the enactment of the 2004 Act on ISS, civil and also criminal liability of ISSPs can be established directly on breach of these specific duties within the 2004 Act on ISS.

In other aspects, the wording of § 3 to 6 of the 2004 Act on ISS is almost identical to that of the ECD, or more precisely identical to the official Czech translation of the ECD. This is not exceptional. Indeed, most of the Member States have also transposed the relevant provisions of the ECD in almost verbatim way. From EU perspective this can be perceived as a positive trend, which produces more intensive harmonisation.

29 Cf. PROLUX Consulting Int., s. r. o. v. Internet Info, s. r. o. (Municipal court in Prague, 17. 3. 2010, č. j. 10 Cm 47/2009-39)
On the other hand, such transposition is often criticised from the perspective of the national legal systems. It is since these mechanical transpositions may bring within national law unnecessary new categories and principles, which might be already present in national law. Although there are no such complications with the ECD transposition in the Czech Republic yet, as it will be shown, it is unfortunate that the legislator did not have courage to describe the so called Notice and Take Down.

1.3. Notice and Take Down

Article 14 ECD, which entails the hosting safe harbour transposed by § 5 of the 2004 Act on ISS, forms legal basis for adoption of the Notice and Take Down ("NTD")\(^{31}\) procedures. According to this provision, ISSP must act expeditiously to remove or to disable access to the information upon obtaining knowledge or awareness of illegal content, in order to preserve immunity. Accordingly, if someone serves notice to the ISSP and thereby the ISSP obtains knowledge or awareness of the illegal content, the ISSP must act expeditiously to remove or to disable access to such content.

A duty to act "expeditiously to remove or to disable access to the information" is also stipulated in respect of caching in Article 13 (1) (e) ECD, and accordingly in § 4 e) of the 2004 Act on ISS. However, this duty arises only upon obtaining actual knowledge that the content was already removed/disabled at the initial source or that an administrative authority has ordered such removal or disablement. Responsibility for UGC in caching services is therefore dependent on the primary hosting activity. Consequently also the notices cannot be served directly by private individuals to ISSP conducting caching. Moreover, other questions which are addressed by this final thesis are not relevant for caching at all or are at rather marginal to caching activity. For example under § 4 e) of the 2004 Act on ISS it is clear, that only administrative authority that may serve the notice is the court. The ISSP also cannot consider truthfulness of such official notice. It follows that caching services are not discussed directly in the final thesis.

In respect of mere conduit, which is protected under Article 12 ECD and accordingly under § 3 of the 2004 Act on ISS, NTD does not apply at all. Mere conduit ISSP merely deals with immediately transient content, and therefore ex-post NTD requirement cannot be applied.\(^{32}\) Mere conduit services are not subjected to duty to remove any content at all for the reason of their fleeting nature.


\(^{32}\) On the other hand such NTD regime might be developed in future under negotiated ACTA agreement in the way that it would actually apply to mere conduit. See Kaminski, M, ‘ACTA’s
To secure that the limitations on liability of ISSPs as described in Part 1.2 are not circumvented by the Member States, Article 15 ECD stipulates that Member States shall not impose any general obligation to monitor the content upon ISSPs. If Member States are left free to impose such obligations, ISSPs would be forced to gain knowledge of illegal information through monitoring and accordingly they would also acquire the liability.\(^33\) Article 15 ECD was implemented by § 6 of the 2004 Act on ISS.\(^34\)

The ECD not only limits liability of ISSPs across the European Union, but as well the ECD attempts to harmonise immunity for different unlawful content. The ECD took the so called horizontal approach. It means that the limitations on liability provided by the Directive are applied in the same manner to all kinds of liabilities, notwithstanding whether they arise from copyright infringement, defamation or even criminal law. It must be noted here, that the final thesis does not address the liability of online intermediaries as such, but only the limitation of liability under the NTD procedure as it was introduced by the ECD.

The Directive intentionally does not regulate NTD itself, but instead in its Recital 40 and Article 16 calls for the Member States to encourage stakeholders to create effective NTD regimes. Not only that the Czech Republic did not show any initiative in this respect, the Czech legislator probably did not realize that EU directives merely provide for goals that need to be achieved by national law and implemented the ECD without elaborating its provisions. It is unfortunate that the Czech legislator has failed to describe or even mention the NTD. The fact that NTD procedure is not described within the Act leaves open too many questions arising with the application of NTD. For example who may serve the notice; whether and to what extent must the notice prove illegality of the content; whether once served notice makes an online intermediary liable for reappearing illegal content etc. Consequently, these inevitable questions have to be answered by the doctrine and ultimately by the courts. The goal of the final thesis is to examine the most important of these questions.

1.4. Thesis questions

The preliminary questions are naturally those on the scope of the 2004 Act on ISS. First, we will ask, who are the subjects that should implement NTD procedures in

---

\(^{33}\) This important provision might be in future hampered by ACTA. See Kaminski, M, ‘ACTA's Digital Enforcement Provisions’ (03 July 2010) <http://balkin.blogspot.com/2010/07/actas-digital-enforcement-provisions.html> accessed 03 July 2010. It seems that this would change NTD into ex ante solution. However, such NTD should rather be called filtering.

\(^{34}\) § 6 of the 2004 Act on ISS: “Poskytovatelé služeb uvedení v § 3 až 5 nejsou povinni a) dohlížet na obsah jimi přenášených nebo ukládaných informací, b) aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace.”
order to avoid liability for UGC? Secondly, in respect of what illegal content can the ISSP rely on the liability limitation? Those are the questions addressed in Chapter 2.

Consequently, when it is clear to whom and to what content NTD regime applies, the questions on the notice itself will arise. Therefore, we will ask, who may serve the notice? What is the required form of the notice and what are the accepted means of serving the notice? Moreover, the content of the notice needs to be scrutinized. What information needs to be in the notice to prove illegality of the respective content? Accordingly, questions on truthfulness of the notice are inevitable. Is there liability for serving untruthful notice? Are the ISSPs obliged to review the truthfulness of the notice? All these difficult questions are addressed in Chapter 3.

When valid notice is served, the ISSP has to act “expeditiously”. Not surprisingly this vague term gave rise to broad discussion, which will be considered in Chapter 4.

Even when a valid notice was served and the ISSP has “expeditiously” taken down the illegal content, the problematic of NTD is not over. Chapter 5 addresses the issue of reappearing illegal content. That is the content that was already taken down, but was again uploaded. This is seen as the Achilles heel of NTD, stressing the fact that NTD is primarily an ex post remedy and cannot itself prevent illegality.

This weakness of NTD regime leads to discussion whether NTD regime is sufficient solution for ISSPs liability for user-generated content and whether ISSPs should be forced to take more proactive approach dealing with illegal UGC. Chapter 6 will describe the main arguments in this discussion in order to set the previous questions that have been asked into the current context.

1.5. Method

As it was explained in Part 1.3, although the e-Commerce Directive in its liability exemptions provides basis for NTD regime, it does not describe NTD procedure at all. Instead, the ECD calls for the Member States and the Commission to encourage drawing of codes of conduct.\(^{35}\) Nevertheless, the ECD itself is at least helpful when defining the scope of this regulation. According to the indirect effect of EU directives, EU directives may serve the national courts as an interpretational tool of national implementing legislation.\(^{36}\) Moreover, under certain conditions EU directives may be even directly applicable. Having in mind, that the ECD immunity regime does not impose any obligations upon individuals, it is submitted that even this direct effect could be invoked if necessary. Therefore, we might examine the application of NTD regime in the Czech Republic by looking at the ECD. Moreover, as it was said, most of the

\(^{35}\) Recital 40 and Article 16 ECD

\(^{36}\) Chalmers, D and Davies, G and Monti, G, European Union law: cases and materials (2\text{nd} edn CUP, Cambridge 2010) 294-300
Member States have implemented the ECD in more or less similar way. Therefore, to understand NTD it will be also helpful to look critically at the implementation of the ECD in other Member States. Useful examples can be found especially in the United Kingdom, Germany and France. In addition to that, the attention will be paid to the rather exceptional Dutch Code of Conduct\(^{37}\) that has been created by stakeholders as it was anticipated in the ECD. Expect that, substantial attention will be given to the NTD regime in the United States under § 512 of the Digital Millennium Copyright Act 1998 ("DMCA"). That is because this provision was the essential inspiration of the ECD. Moreover, the DMCA actually provides for NTD in detail and therefore could still provide valuable inspiration for the courts applying the 2004 Act on ISS.

1.6. Assumptions

Author is convinced that NTD regime is principally a good solution to liability of online intermediaries for illegal user-generated content. Moreover, this solution is appropriate in Web 2.0 environment. That is because NTD is essentially a “Web 2.0 tool”. Under NTD regimes, the notices are served by the users themselves and not by some central supreme authority. In other words, notices are “user-generated” similarly to the content of Web 2.0. The courts or the enforcement bodies step in only as an ultimate solution, when dispute arises. This means that NTD is essentially a Web 2.0 concept and therefore NTD offers at least partial solution to the illegal UGC in Web 2.0 environment.

The final thesis will try to provide comprehensible information that will support future applicability of NTD within the Czech Republic. In this respect, it should be bear in mind that, although NTD seems as a logical approach, it was not adopted all over the world. Especially outside the western civilisation area\(^{38}\) the approaches to liability of online intermediaries differ significantly.\(^{39}\)

2. SCOPE

The 2004 Act on ISS is in force since 7 September 2004 and apparently there have not arisen any difficulties in respect of its application in time. The thesis also does not elaborate territorial applicability, which is in the field of internet law an extensive topic on its own. Instead, we are going to describe, who the so called Information


\(^{38}\) For our purposes western civilisation countries are: Canada, U.S.A., member states of European Economic Area with Switzerland, Australia and New Zealand.

\(^{39}\) For recent example see ‘Google faces Brazil fine for providing forum in which defamation could take place’ (OUT-LAW News, 27 April 2010) <http://www.out-law.com/page-10970> accessed 11 June 2010
society service providers are, in order to learn who the subjects of the 2004 Act on ISS are. Secondly, we need to explain what the hosting service is, because that is the only service that NTD is applied to. Thirdly, we are going to consider in respect of what content the ISSP can rely on the immunity regime.

2.1. Information society service provider (“ISSP”)

The safe harbour in Article 14 ECD similarly to Articles 12 and 13 ECD applies to the “service provider”, in Czech “poskytovatel sluţby”. The e-Commerce Directive defines the service provider in Article 2 (b) ECD as “any natural or legal person providing an information society service”. The Czech definition in § 2 d) of the 2004 Act on ISS is identical.40 Therefore, service provider in the sense of the ECD is more precisely “information society service provider” (“ISSP”).

To further elaborate the definition of service provider from Article 2 (b) ECD, which is identical to ISSP, we need to define the “information society service” (“ISS”). The ECD was adopted to secure the free movement of information society services between the Member States (Article 1 (1) ECD). The ECD defines information society services in its Article 2 (a) by reference to the definition in Article 1 (2) of the Technical Standards and Regulations Directive (“TSRD”)41 that provides:

*Information Society service...[is]...any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.*

The TSRD then further specifies this crucial definition:

- “at a distance” means that the service is provided without the parties being simultaneously present,
- “by electronic means” means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,
- “at the individual request of a recipient of services” means that the service is provided through the transmission of data on individual request.

This definition of ISS was with insignificant differences transposed to the Czech legal system through § 2 a) of the 2004 Act on ISS.42 However, the TSRD and also the

---

40 § 2 of the 2004 Act on ISS: “Pro účely tohoto zákona se rozumí...d) poskytovatelem sluţby kaţdá fyzická nebo právnická osoba, která poskytuje některou ze sluţeb informační společnosti”.
42 § 2 of the 2004 Act on ISS: “Pro účely tohoto zákona se rozumí...a) sluţbou informační společnosti jakákoli sluţba poskytovaná elektronickými prostředky na individuální žádost uţivatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; sluţba je
ECD provide more specific guidance for definition of the ISS. These will be now described. In accordance with the principle of indirect effect of EU directives, this further guidance in the directives must be followed by the national courts, when interpreting § 2 a) of the 2004 Act on ISS.

Article 1 (2) of the Technical Standards and Regulations Directive provides that the TSRD does not apply to radio broadcasting services and television broadcasting services. However, it is clear that these cannot be regarded as ISSP since they are not provided at the individual request of a recipient of services. More importantly Article 1 (2) TSRD provides that certain services are not to be considered as ISS, because they do not fulfill one of the three above enumerated requirements. They are not provided "at a distance", "by electronic means" or "at the individual request of a recipient of services". Article 1 (2) TSRD points to an indicative list of such services in Annex V of the TSRD:

**Indicative list of services not covered by the second subparagraph of point 2 of Article 1**

**1. Services not provided "at a distance"**

Services provided in the physical presence of the provider and the recipient, even if they involve the use of electronic devices

(a) medical examinations or treatment at a doctor's surgery using electronic equipment where the patient is physically present;
(b) consultation of an electronic catalogue in a shop with the customer on site;
(c) plane ticket reservation at a travel agency in the physical presence of the customer by means of a network of computers;
(d) electronic games made available in a video-arcade where the customer is physically present.

**2. Services not provided "by electronic means"**

Services having material content even though provided via electronic devices:

(a) automatic cash or ticket dispensing machines (banknotes, rail tickets);
(b) access to road networks, car parks, etc., charging for use, even if there are electronic devices at the entrance/exit controlling access and/or ensuring correct payment is made,
(c) plane ticket reservation at a travel agency in the physical presence of the customer by means of a network of computers;
(d) electronic games made available in a video-arcade where the customer is physically present.

Off-line services: distribution of CD roms or software on diskettes,

Services which are not provided via electronic processing/inventory systems:

(a) voice telephony services;
(b) telefax/telex services;
(c) services provided via voice telephony or fax;
(d) telephone/telefax consultation of a doctor;
(e) telephone/telefax consultation of a lawyer;
(f) telephone/telefax direct marketing.

**3. Services not supplied "at the individual request of a recipient of services"**

Services provided by transmitting data without individual demand for simultaneous reception by an unlimited number of individual receivers (point to multipoint transmission):

(a) television broadcasting services (including near-video on-demand services), covered by point (a) of Article 1 of Directive 89/552/EEC;

poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat".

43 Television broadcasting is defined in Point (a) of Article 1 of Directive 89/552/EEC as "the initial transmission by wire or over the air, including that by satellite, in unencoded or encoded form, of television programmes intended for reception by the public. It includes the communication of programmes between undertakings with a view to their being relayed to the public. It does not include communication services providing items of information or other messages on individual demand such as telecopying, electronic data banks and other similar services".
(b) radio broadcasting services;
(c) (televised) teletext.

In addition to limitations in Article 1 (2) TSRD, the ECD also expressly excludes certain services from its scope. Article 1 (5) ECD provides that the Directive does not apply to:

(a) the field of taxation;
(b) questions relating to information society services covered by Directives 95/46/EC and 97/66/EC;
(c) questions relating to agreements or practices governed by cartel law;
(d) the following activities of information society services:
   - the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority,
   - the representation of a client and defence of his interests before the courts,
   - gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

Moreover, the ECD in its Recital 17 explains that the referred definition of ISS in the TSRD covers “any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service”. This explanation therefore specifies the original definition from the TSRD in respect of “electronic means”, which are described as “means of electronic equipment for the processing (including digital compression) and storage of data”. However, it is dubious that this specification provides more clarity.

The ECD is more helpful in its Recital 18, which specifically lists, which services are ISS and which are not:

*Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line; activities such as the delivery of goods as such or the provision of services off-line are not covered;*

*information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data;*

*information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service;*

*television broadcasting within the meaning of Directive EEC/89/552 and radio broadcasting are not information society services because they are not provided at individual request; by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services;*

*the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service;*
activities which by their very nature cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient are not information society services.

Interestingly enough, even more specific was the Commission in its comment on adoption of the ECD. The commission stated that the ECD covers among others:

on-line newspapers, on-line databases, on-line financial services, on-line professional services (such as lawyers, doctors, accountants, estate agents), on-line entertainment services such as video on demand, on-line direct marketing and advertising and services providing access to the World Wide Web.\(^4^\)

These helpful non-binding provisions and statements show among others, that the requirement that service must be “normally provided for remuneration” is to be interpreted in a very broad sense. The aim of the ECD is naturally to improve functioning of internal market,\(^4^5\) which is inherent to the very existence of European Union and its competence. The ECD secures better functioning of the internal market through supporting cross-border e-commerce. Accordingly, the ECD applies only to commercial services, in other words to services that are normally provided for remuneration. However, on national level, there is no reason, why entirely free services that do not profit even from advertisements, should be excluded from the protection. Similar conclusion was already reached by several courts within the European Union. For example Wikipedia, which is run by non-profit foundation, has enjoyed the protection of safe harbour in French libel case,\(^4^6\) and similarly a provider of free discussion forum has availed the protection in Germany.\(^4^7\) Therefore, it is submitted that the requirement that the service is normally provided for remuneration can be satisfied by virtually any activity that is carried out online. The requirement therefore does not limit the scope of the 2004 Act on ISS.

However, limitation on application of hosting safe-harbour is in Article 14 (2) ECD, which provides that the safe-harbour does not apply when the recipient of the service is acting under the authority or the control of the provider. That is because in such situation the ISSP has again, although indirectly, control over the content and therefore he does not deserve immunity. This exemption covers especially employment relationships. However, this provision was used by the courts in France to refuse rather deserved protection to on-line auction website eBay for sale of counterfeits by its


\(^4^5\) Recitals 1-7 ECD


\(^4^7\) OLG Düsseldorf from 07.06.2006, I-15 U 21/06 in Polčák, R, Právo na internetu - Spam a odpovědnost ISP (Computer Press, 2007) 71
The court reasoned that since eBay has controlled the presentation of the web pages and also derived profits from the transactions concluded between its users, it could not avail hosting protection, which requires mere passive nature of the ISSP. Such interpretation appears misguided, since it would in its consequence entirely ruin the granted protection. It would mean that almost any provider of Web 2.0 services would be seen as having control over its users and thereby lose its immunity.

Furthermore, in determination of the scope of the ECD it should be mentioned that Article 1 (4) ECD provides that the Directive does not establish additional rules on private international law nor does it deal with the jurisdiction of Court, and Article 1 (6) ECD that the Directive does not affect measures taken at Community or national level, in the respect of Community law, in order to promote cultural and linguistic diversity and to ensure the defence of pluralism. Consequences of these limitations are still to be seen.

2.2. Hosting

Having defined ISSPs and setting out areas/services that are excluded from the scope of the e-Commerce Directive, in order to fully understand the scope of the ECD, it must be bear in mind that NTD regime is applied only to the hosting (Article 14 ECD). Therefore, no other activity, even if it concerns information society service, can benefit from this particular safe harbour.

According to Article 14 (1) ECD, hosting exemption applies to the storage of information provided by a recipient of the service and stored at the request of a recipient of the service. Similar definition of “hosting” can be found also in § 5 of the 2004 Act on ISS.

Content aggregators, search engines and providers of hyperlinks cannot be anchored in any of the three described safe harbours. The closest category is the hosting, which provides for “storage of information”. However, content aggregators, search engines and providers of hyperlinks do not store the content, but merely navigate to it. Although, these online intermediaries fall within the definition of ISSP,

48 cases S.A. Louis Vuitton Malletier v eBay Inc., Tribunal de Commerce de Paris, Premiere Chambre B (Paris Commercial Court), Case No. 200677799; Hermès’s International v Mme Cindy F., eBay France and eBay International AG, Tribunal de Grande Instance de Troyes; and Christian Dior Couture, SA v eBay Inc. (RG No.: 2006077807), Paris Commercial Court, 1st Chamber, Division B, in Wong, H, Ch, ‘eBay's liability for counterfeits: a transatlantic comparison’ (2009) 5 JIPLP, 3-4

49 Most significant on this topic are disputes around Google news. For more see Belgian case Google v. Copiepresse, No. 06/10.928/C (Tribunal de premiere instance de Bruxelles) or discussion on Ruppert’s Murdoch quarrel with Google News <http://www.guardian.co.uk/media/2009/nov/09/murdoch-google> accessed 21 December 2009

50 Search engines have been generally successful in keeping immunity. e.g. Metropolitan v Designtechnica Corp. [2009] EWHC 1765 (QB) found that search engine cannot be a publisher at common law and therefore cannot be liable for defamatory material to that it links.
they are not protected under the ECD,\(^{51}\) since their activities do not fit into any of the categories established by the e-Commerce Directive (hosting, caching, mere conduit).\(^{52}\)

Having in mind that those ISSPs exercise even less legal and factual control over the disputable content, and consequently having even less knowledge about its illegality, it seems logical that they should enjoy at least the same level of immunity as other ISSPs, who transmit, cache or host the content.

The DMCA calls these services as Information Location Tools and provides them with similar safe harbour as hosting services.\(^{53}\) Spain, Portugal and Austria followed that example and having in mind the crucial role that search engines and hyperlinks play in navigation throughout the internet these three Member States have provided those categories of services with special safe harbours.

It should be the legislator to remedy this significant loophole in Czech law in the future. Till then, courts, for the reasons given above, should apply safe harbours \textit{a maiori ad minus} to the content aggregators, search engines and providers of hyperlinks. If hosting of the illegal content is not illegal in particular situation, it should not be illegal to help localize such content (of course automatically and unintentionally). Most important for constructing such analogous safe harbour are rules set out in Article 14 ECD for hosting. These provide that the ISSP is not liable for UGC as far as he does not have actual knowledge of illegal activity, or for the purposes of claims for damages “is not aware of facts or circumstances from which the illegal activity or information is apparent”.\(^{54}\) Moreover, the ISSP must act “expeditiously to remove or to disable access to the information” upon obtaining such knowledge or awareness.\(^{55}\)

Dutch Code of Conduct in this connection talks about “scaling up”. It means in situations when website provider cannot be contacted or does not respond, the notifier may turn to the hosting provider (ISSP, which physically hosts the particular website), or if even he cannot be contacted or does not respond, the notifier may turn to the internet access provider and ultimately to the physical access provider (cable/glass fibre).


\(^{52}\) Edwards, L and Waelde, C, (eds), \textit{Law and the Internet} (3rd edn Hart Publishing, Oregon 2009) 77

\(^{53}\) § 512 (d) DMCA

\(^{54}\) Article 14 (1) (a) of the e-Commerce Directive

\(^{55}\) Article 14 (1) (b) of the e-Commerce Directive
2.3. **Object (content)**

Having defined which services are covered by the e-Commerce Directive regime, it must be set out in respect of what content can an ISSP rely on it. It is not important from the legal point of view, whether the illegal content is in a form of text, picture, sound or video. Important is, what laws are infringed by the content. In other words, what kinds of illegality are covered by the ECD?

The ECD takes horizontal approach. It means that the safe-harbours generally cover all types of illegal content that may appear on the internet. Similarly the 2004 Act on ISS does not indicate what kinds of illegality are covered. Therefore, the 2004 Act on ISS covers every possible illegal activity that can be carried out through information society services of online intermediaries.

Although the protective liability regime does not make any difference between for example defamation and child pornography, there will be practical differences as we will see in Part 3.3. The ECD horizontal approach may be contrasted with United States’ vertical approach. In the United States, NTD regime applies specifically only to copyright infringement under the DMCA.

It should also be noted that the ECD covers both, civil and criminal liability. This was confirmed in the First Report on the application of Directive 2000/31/EC. However, the Directive itself is not entirely clear in this respect. Recital 8 ECD, which provides that the objective of the Directive “is to create a legal framework to ensure the free movement of information society services between Member States and not to harmonise the field of criminal law as such.” In other words, although the Directive regulates criminal law, it does not intend to harmonise it. However, it should be also barred in mind that in criminal law, mens rea is necessary and therefore it is inevitable that guilty online intermediary have actual knowledge of illegal UGC.

Exceptions to the above explained general applicability of the Directive in respect of different areas of law may be found in already mentioned Article 1 (5) ECD, which provides that the Directive shall not apply to:

1. **the field of taxation**,
2. **questions relating to information society services covered by Directives 95/46/EC and 97/66/EC**,
3. **questions relating to agreements or practices governed by cartel law**;

---


58 Currently a very controversial criminal proceeding is taking place in Italy against four Google employees, who did not have knowledge of the illegal content, but are being prosecuted for failure to comply with privacy laws. See fn. 62
(d) the following activities of information society services:
- the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority,
- the representation of a client and defence of his interests before the courts,
- gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

With respect to the application of NTD, and in accordance with the current development of the internet and the law, most important exception appears to be so far point (b), which refers to the Data Protection Directive\textsuperscript{59} and to the Directive 97/66/EC,\textsuperscript{60} which was repealed by the Directive on privacy and electronic communications.\textsuperscript{61} Article 1 (5) (b) ECD excludes the area regulated by the Data Protection Directive and the Electronic Privacy and Communications Directive from the scope of the ECD. This has recently stirred a lot of controversy, since it seemed to be the reason why Italian court could held criminally liable four Google employees for user uploaded video of bullied kid, although Google has removed the video within hours from proper notification and the employees did not have any knowledge about the video. It was argued that there is no reason why the ECD excludes from its scope data protection area, because the mentioned directives do not regulate same issues. Therefore it was suggested that the ECD is amended in this respect and the exclusion abolished.\textsuperscript{62} However, it seems now that this was not the reason behind the controversial ruling.\textsuperscript{63} Moreover, it is highly probable that the ruling will be reversed on appeal. Still, this well illustrates the extent of uncertainty surrounding the application of the ECD regimes. On the other hand, the ECD regime was successfully relied upon in case on violation of privacy in France. In this case sexual orientation was revealed on Wikipedia, which taking down the content, successfully claimed protection under French law implementing the ECD.\textsuperscript{64} Since none of the above mentioned exclusions were transposed to the 2004 Act on ISS, it appears that ISSPs can truly rely upon the act in respect of any illegal activity.

\textsuperscript{59} Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
\textsuperscript{60} Directive 97/66/EC of the European Parliament and the Council of 15 December 1997 concerning the processing of personal data and protection of privacy in the telecommunications sector, OJ L24/1 of 30/1/98
\textsuperscript{62} Robertson, S, ‘Google convictions reveal two flaws in EU law, not just Italian law’ March 2010 <http://www.out-law.com/page-10805> accessed 18 June 2010
3. THE NOTICE

The ECD remains utterly silent in respect of any issue related to the notice. The ECD simply stipulates that the ISSP upon obtaining knowledge or awareness as specified in Article 14 (1) (a) ECD, acts expeditiously to remove or to disable access to the information.

3.1. Who may serve the notice

Since the 2004 Act on ISS remains utterly silent about the notice\textsuperscript{65} and nothing else indicates otherwise, it appears that everybody is entitled to serve the notice. Similar conclusion may be reached for example in France,\textsuperscript{66} Germany\textsuperscript{67} or in the United Kingdom.\textsuperscript{68}

Contrary to that, in Italy Article 16, letter b) of the Decreto legislativo n 70, 9 April 2003, stipulates that the ISSP is required to act promptly to remove the information or to limit the access to it, only when “he obtains actual knowledge, upon notification from the competent authorities”.\textsuperscript{69} Therefore, the ISSP in Italy must act only when they are notified by the “competent authority” and on the other hand may ignore notifications from others. However, this clearly stems from incorrect reading of the ECD. Articles 13 and 14 ECD according to their paragraphs 2 and 3 respectively, do not affect the possibility of a national court or administrative authority (in other words “competent authorities”), of requiring the ISSP to terminate or prevent an infringement. A contrario NTD regime established in Articles 13 and 14 is clearly designated to be used by private individuals and not exclusively by certain public “competent authorities”. The Italian approach ruins the praised “Web 2.0 aspect” of NTD.

Although, it is clear that Italian restrictive approach is incorrect, the opposite broad approach, which was adopted by the majority of the Member States including the Czech Republic, is neither optimal. Regime that allows anybody to serve the notice creates a substantial risk that NTD procedure is abused. Serving false notices might be an elaborate tool of unfair competition or simple revenge in private disputes. The risk of abuse is even worse because the notices do not have to include contact details of the notifier and can be therefore easily served under false identity or anonymously.

\textsuperscript{65} § 5 (1) b) of the Act No. 480/2004 Coll. on certain information society services
\textsuperscript{66} see Article 6.1.5 of Loi 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique
\textsuperscript{67} § 10 and 11 of the Gesetz über die Nutzung von Telediensten (Teledienstegesetz – TDG) from 22 July 1997
\textsuperscript{68} ss 18, 19 and 22 of the The Electronic Commerce (EC Directive) Regulations 2002 SI 2002/2013
Therefore, under the American DMCA only aggrieved parties and their agents can serve the notice. It follows that the DMCA notice must be signed physically or electronically by the owner of an exclusive right that is allegedly infringed or by a person authorized to act on his behalf.\footnote{\$ 512 (c) (3) (A) (i) DMCA} Moreover, the DMCA notice must contain “information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.”\footnote{\$ 512 (c) (3) (A) (iv) DMCA}

If we take into account that the DMCA deals only with copyright infringement, this is certainly sensible approach. Copyright protection is primarily in the interest of copyright holders. Taking into account core principle of civil law that \textit{vigilantibus iura scripta sunt}, it is natural that only the aggrieved party is permitted to serve the notice. This practice brings much more certainty to the online intermediary when assuring that the notice is truthful. Moreover, it would be difficult for other persons than the aggrieved party in copyright cases to sufficiently prove that the content is actually illegal, in other words that the content is disseminated without the consent (license) of the owner. The fact that the notice is served by the authorised person, assures that the notice is not served under false identity. Overall, this limitation of entitled persons prevents abuse of NTD.

On the other hand, the 2004 Act on ISS being horizontally applicable covers also large amount of illegal material that is notified in public interest, e.g. content of racial hatred, child pornography or other criminal activity. Therefore, it is desirable that anyone can serve the notice in respect of such material. The aggrieved party in those cases is the society as a whole.

However, the notices should not be served anonymously. Accordingly in France, it is not possible to serve the notice anonymously. Art 6.I.5 requires that the notice includes the general information about the person notifying.\footnote{Casarosa, F, ‘Wikipedia: Exemption from Liability in Case of Immediate Removal of Unlawful Materials’, (2009) 6 SCRIPTed 669, <http://www.law.ed.ac.uk/ahrc/script-ed/vol6-3/casarosa.asp> accessed 04 July 2010, 673 fn 20} In the United Kingdom, it is not forbidden. However, ECD Regulation\footnote{The Electronic Commerce (EC Directive) Regulations 2002, SI 2002/2013, which incorporate the ECD into the law of the United Kingdom.} 22 (b) (i) directs courts to consider, whether the notice included the full name and address of the sender of the notice. That means that anonymous notice in the United Kingdom may be found by the court as ineffective.

The 2004 Act on ISS remains silent about the notice and does not provide any guidance for courts. Consequently, the notice can be served by anyone and even anonymously.\footnote{Polčák, R, \textit{Právo na internetu - Spam a odpovědnost ISP} (Computer Press, 2007) 68-69} However, it should be noted that anonymity will significantly reduce the
credibility of the notice. Consequently, in certain circumstance even in the Czech Republic, anonymous notice might not factually inflict the required knowledge of the ISSP about the illegal content. In that case the notice would be considered by courts as ineffective.

3.2. Form of the notice

What is the required form and where should the notice be served? Since the 2004 Act on ISS does not describe the notice at all, there are no formal requirements on the notice and no definite answers for these questions. Indeed, the way how the ISSP learns about the illegal content does not have to be the notice at all. However, some basic rules need to be pursued, in order to serve an effective and valid notice.

First, in respect of form of the notice, the written form seems preferable. In the United States physical or electronic written form is expressly required by § 512 (c) (3) DMCA. Although, in the United Kingdom the written form is not mandatory, it is at least preferable according to the law. British ECD Regulation 22 (a) provides that a court should take into account among other things “whether a service provider has received a notice through a means of contact made available in accordance with regulation 6 (1) (c)”. The referred ECD Regulation 6 (1) (c) demands that ISSPs makes available among other thing: “his electronic mail address, which make it possible to contact him rapidly and communicate with him in a direct and effective manner”.

In addition, as we have seen, email is an alternative to physical written form and in ECD Regulation 6 (1) (c), email seems to be preferred. Probably not only because of its immediate nature, but also having in mind that the ISSP will have to localize through often long internet addresses all the infringing content in order to remove it, email will be always most appropriate way of serving the notice.

The second crucial question is, where should be the notice addressed? In this respect we may follow Article 5 ECD, which also requires the ISSP to make “easily, directly and permanently” available certain types of self descriptive information. These include:

(a) the name of the service provider;  
(b) the geographic address at which the service provider is established;  
(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner.

Especially letter (c) of Article 5 ECD is clearly intended to secure communication point for purposes of serving the notice. Even stricter is in this respect the DMCA regime. In the United States it is actually necessary that the online intermediary registers an agent for notifications with the US Copyright Office. Otherwise, the online
intermediary is not eligible for the protection of the DMCA safe harbour.\textsuperscript{75} Similarly, in case such information is not provided by the ISSP as demanded by Article 5 (c) ECD, the ISSP could theoretically disqualify itself from the protection of the ECD. This would clearly be the conclusion, if there was no possibility whatsoever, to contact the ISSP. However, this requirement was not transposed into the Czech law. Therefore, it might be disputable, whether ISSPs in the Czech Republic are under duty to provide their contact details. Certainly at least persons carrying out business are under duty to state their name and place of business on their websites (§ 13a\textsuperscript{76} of the Commercial Code\textsuperscript{77}).

It will be in the interest of the notifier, to serve the notice in writing. In that way, sufficient proof that the notice was served, is retained. Paragraph 5 (1) b) of the 2004 Act on ISS demands that the fact, that the ISSP has learned (gained knowledge) about the illegal content, is “verifiable”. Therefore, the written form seems inevitable. At the same time it is obvious that electronic means, such as email or electronic form on provider’s website, might be used instead of mail. Indeed, for their expeditious nature, electronic means will be preferred by the notifiers, but as well by the ISSP, for whom it will be easier to precede such notices.

The conclusion is that in the Czech Republic the notice should be served in writing and to the address that was provided for that purpose. For example, it is not sufficient to serve the notice through comment under allegedly illegal video. The ISSP does not have to monitor the discussion and therefore might not learn about such notice at all. However, in case the notice was not served in writing or was not served to the provided electronic or physical address, but the ISSP actually receives the notice, the ISSP still have to take all the steps that can be demanded from him.

\textbf{3.3. Necessary information}

Again, most of the Member States together with the Czech Republic did not specify the necessary information that must be in an effective notice. Therefore, every notice must be considered individually in order to determine according to § 5 of the 2004 Act on ISS, whether it contains enough information to cause actual knowledge of illegal nature of content or about illegal activity of the user on the side of the ISSP.

\textsuperscript{75} § 512(c)(2) DMCA
\textsuperscript{76} This provision transposes First Council Directive 68/151/EEC of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community
Fortunately, some of the Member States did not hesitate to at least provide certain guidance. For example, we have already mentioned Britain’s ECD Regulation 22, which provides that the court shall have regard among others to:

... 

(b) the extent to which any notice includes -

(i) the full name and address of the sender of the notice;
(ii) details of the location of the information in question; and
(iii) details of the unlawful nature of the activity or information in question.

In France according to Article 6.I.5 of Loi 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique, following information must be included in the notice, in order to reach the presumption of knowledge of the ISSP:

- the date of notification;
- the general information about the person notifying;
- the description of the presumed unlawful materials;
- and the motivation for the removal of the materials with a reference to legal provisions.\(^78\)

Section 512 (c) (3) (a) DMCA in the United States requires that following information is included in the notification of claimed infringement:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Dutch Code of Conduct requires that “the report” (that is the notice) includes:

- the contact details of the notifier;
- the information that the intermediary needs to be able to evaluate the content, at least including the location (URL);
- a description of why the content is unlawful according to the notifier, or why it is in conflict with the criteria published by the intermediary governing undesirable content;
- a statement of the reason why this intermediary is being approached as the most appropriate intermediary to deal with the matter.

Interestingly enough, Dutch Code of Conduct also requires that “a statement of the reason why this intermediary is being approached as the most appropriate intermediary to deal with the matter” is also included in the notice. However, it is submitted that this information does not seem necessary under Czech law. As far as the ISSP is able to remove/disable the notified content, the ISSP must do so, notwithstanding the fact that there is some other, more appropriate ISSP. Moreover, in most cases it will be abundantly clear why particular ISSP, usually in the position of a website owner, is most appropriate to remove/disable the particular content.

Expect the importance of identification of the notifier, which we have already discussed in Part 3.1, those various regulations indicate that following information is necessary in order to serve an effective notice: identification and location of the information, reason of claimed illegality. Moreover, it is submitted that the notifier need to submit “proof” of content’s illegality where illegality is not apparent from the content itself. Typically in case of defamatory material it is necessary to argue why the information is false and therefore is defamatory. Clearly, these are the information that must be provided also in the Czech Republic. Otherwise, the ISSP could not gain knowledge of the content’s illegality. The fact that the notifier claims that the content is illegal does not itself render ISSP’s knowledge of content’s illegality.

At the first sight, the requirement of identification and location of the information does not seem to cause any difficulties. The notifier simply needs to submit the specific URL address of the illegal content. On the other hand, it will not be sufficient if the notifier merely notifies the ISSP that there is illegal information on the particular web, but does not specify what information and where exactly. In other words, pointing merely to the top-level URL will not be sufficient.79 The ISSP cannot be forced to seek for the illegal content. Specific address is therefore necessary. Moreover, in PROLUX v. Internet Info,80 which concerned internet discussion, the defendant argued that it is necessary that the notice specifies individual comments that are illegal and need to be removed. That is since it would be unreasonable to remove whole discussion thread because of for example single illegal comment. This argument is certainly valid and in similar cases the identification of particular illegal content should not cause any difficulties to the notifier. However, the Municipal Court that has ruled in first instance did not address this concern, and ordered that the whole discussion thread is removed. However, the case is currently in appeal.

79 Such conclusion was reached in the United States in Perfect 10, Inc. v. Google, Inc. No. CV 04-9484 AHM (SHx) (26 July 2010)
80 PROLUX Consulting Int., s. r. o. v. Internet Info, s. r. o. (Municipal court in Prague, 17. 3. 2010, č. j. 10 Cm 47/2009-39)
The second requirement, that proof of unlawfulness is submitted, is much more complicated and may cause more practical difficulties. What information needs to be in a notice to prove illegality of the content? Certain types of illegality are usually apparent from the content itself. For example child pornography, expressions of racial hatred or threats are illegal at first sight. Therefore, the mere location of such content should inflict ISSP’s knowledge of the illegality. As Polčák argues, *ignoratia legis neminem excusat*, consequently the ISSPs are presumed to know the law and should recognise such apparently unlawful content.\(^{81}\) It will be sufficient to notify the ISSP about the location of such content, without providing him with further information what rules are being violated etc.

### 3.4. Truthfulness of the notice

To what extent should the ISSP review truthfulness of the notice, or in other words to what extent can the ISSP rely in a good faith on the notice? In order to avoid misuse of NTD and to ease the position of ISSPs, who have to decide whether to remove the notified content or not, it is necessary to impose liability for false notice upon the notifier. That is the reason why for example § 512 (f) DMCA holds liable any person that knowingly materially misrepresents under section § 512 DMCA.\(^{82}\) Knowing that the notifier is liable for the notice, it is easier for the online intermediary to rely on the truthfulness of the notice. Moreover, § 512 (g) (1) DMCA protects the online intermediary from any claims based on the online intermediary’s good faith disablement or removal of the content.\(^{83}\) So if the online intermediary removes or disables the content in a good faith, believing that the content is illegal, the content provider does not have a claim against him. Therefore, the online intermediary is protected from “both sides”, from the notifier and also from the content provider. At the same time, the content provider can protect his rights by the so called put-back procedure. It means that according to § 512 (g) (3) DMCA the content provider, whom the online intermediary must inform about the take-down,\(^{84}\) can serve a counter notification to the online intermediary. Following the counter notification, the online intermediary must inform the notifier and put back the disputed content (§ 512 (g) (2) (C)) after ten business days following receipt of the counter notice, unless the original notifier has

---

\(^{81}\) Polčák, R, *Právo na internetu - Spam a odpovědnost ISP* (Computer Press, 2007) 70

\(^{82}\) Therefore § 512 (c) (3) (A) DMCA requires that the notifier includes in the notification (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law. And (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

\(^{83}\) Similarly the Dutch code of conduct in 4 d. provides the ISSP with an option to request an explicit indemnity from the notifier against claims from the content provider.

\(^{84}\) § 512 (g) (2) (A) DMCA
informed the ISSP that he has filed an action seeking a court order against the content provider. All these provisions efficiently secure that the NTD is not misused by intentionally false notices.

There are no such provision in the ECD and neither in the 2004 Act on ISS. However, this does not mean that liability of the notifier cannot be derived from other legal norms. In the Czech Republic the notifier, who intentionally serves false notice, could be held liable under § 424 of the Civil Code, which stipulates that a person who caused damage by an intentional conduct against good manners shall be liable for it. On the other hand, we shall not forget that in the Czech Republic the notice can be effectively served anonymously. Consequently, it may be very hard to find out and held liable the person serving the false notice.

In respect of immunity of the ISSP against the content provider, the ISSP can limit such liability in the contract that he enters into with the content provider. However, even this private limitation must be within certain limits and the ISSP cannot remove content arbitrarily. As Recital 46 ECD indicates, the ISSP must undertake the removal or disablement “in the observance of the principle of freedom of expression and of procedures established for this purpose at national level”. So far there are no procedures established for this purpose at national level within the Czech Republic. However, freedom of expression is stipulated in Article 17 of Charter of Fundamental Rights and Basic Freedoms and the ISSPs, having control over the communication on the internet, clearly cannot interfere with this right. It follows that the ISSP can remove the notified content only if he is in a good faith that the content is illegal.

4. DUTY TO ACT EXPEDITIOUSLY

Section 5 (1) b) of the 2004 Act on ISS provides that the ISSP would be liable if “he did not expeditiously take all the steps, which could be demanded from him, to remove or to disable the access to the information” upon learning about the illegal nature of the information. But how expeditiously is expeditiously?

Article 14 (1) b ECD does not provide an answer. It merely provides that the ISSP must act “expeditiously to remove or to disable access to the information” upon obtaining knowledge or awareness of illegal content. Similar wording can be found in § 512 (c) (1) (C) DMCA, which requires online intermediary to “respond expeditiously”.

---

85 Polčák, R, Právo na internetu - Spam a odpovědnost ISP (Computer Press, 2007)
86 Act No. 2/1993 Coll.
87 § 5 (1) b) of the 2004 Act on ISS: “dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodelal něčím veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.”
The ECD is sometimes criticised for not providing more specific guidance here.\textsuperscript{88} However, author is convinced that it is desirable that this term leaves discretion to the judges to decide what is expeditious in individual cases. Depending on the circumstances of the case, it could be minutes, days or even weeks.

Moreover, it is welcomed that the Czech legislator has made this duty dependent on subjective criteria. The ISSP under Czech regime has to take only such steps, “which could be demanded from him”. It means that ultimately the courts will have to decide what steps could have been demanded from the particular ISSP in the particular case, and moreover how expeditiously such steps ought to have been taken.

Following facts will inevitably come into consideration. First, the size and the resources of the ISSP will determine the steps that might be expected from the ISSP. Surely there will be difference between large companies and for example enterprises that are operated by a single person. The latter one could hardly be demanded to process notices five or even seven days a week. Also smaller enterprises could be hardly expected to seek expensive legal advice. Moreover, less strict approach may be taken towards non-profit organisations that simply do not have resources for expeditious processing of notices. Secondly, it is the nature of the reported content and the amount of the reported content. Especially, whether the notice points to unequivocally illegal content, or whether more information is necessary to establish illegal nature of the content. For example in cases of terrorist related material the British specialised Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007 provides for two-day period in which the noticed illegal content that encourages terrorism must be taken down. The time limit can be exceeded only in case there was a “reasonable excuse”.\textsuperscript{89} On the other hand, Libel Bill proposed by Lord Lester provides for fourteen-day period in respect of libel related content.

It is also interesting to note that section 4 c. of the Dutch Code of Conduct provides that the notifier can request that the ISSP deals with the notice urgently. Naturally the notifier needs to explain the reasons for that. It is submitted that sufficient information about urgency of the issue in the notice may theoretically influence court’s final decision in the Czech Republic as well.

5. REAPPEARING ILLEGAL CONTENT

Can once served notice make the ISSP liable for reappearing illegal content? By reappearing content we mean content that has been once taken down, but was

\textsuperscript{88} Edwards, L and Waelde, C, (eds), \textit{Law and the Internet} (3\textsuperscript{rd} edn Hart Publishing, Oregon 2009) 66
uploaded again, maybe even to the very same location and by the very same user. It is not possible to find a direct answer to this question in the ECD or in the 2004 Act on ISS. On the other hand, the American DMCA is quiet specific on this issue. Section 512 (i) (1) (A) DMCA requires online intermediaries to implement a “policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers”. It effectively means, as it was already confirmed by the courts, that online intermediaries are under duty to track infringement incidents, and if these are repeated, the online intermediaries have to terminate the access of repeat infringers.\(^9^0\) Therefore once served notice can have effect in respect of future content within the American jurisdiction.

The 2004 Act on ISS does not entail similar requirement and does not stipulate any duty in respect of the reappearing content. Therefore, simple literal interpretation of of § 5 of the 2004 Act on ISS leads us to the conclusion that notice establishes ISSP’s duty to act only in respect of the currently existing and notified content. Accordingly, an ISSP cannot be held liable for reappearing illegal content, unless notified. However, we shall not forget that the 2004 Act on ISS in line with the ECD demands not only that an ISSP does not have actual knowledge of the illegal content, but also in its § 5 (1) a) that the ISSP with regard to the nature of his activity and circumstances and nature of the case, could have known that the content of stored information or activity of the user are illegal. It is apparent that such awareness in particular cases may arise out of the fact that similar content (same information or same user) was already notified before reappearing.

On the other hand it may be argued that Article 15 ECD, transposed by § 6 of the 2004 Act on ISS, forbids imposition of general obligation to monitor upon ISSPs. However, Recital 47 ECD confirms that Article 15 ECD “does not concern monitoring obligations in a specific case”. It follows that the ECD does not prohibit imposition of a duty upon an ISSP to monitor activity of the particular user, who has already indulged in an illegal activity.

This conclusion was also reached by famous “Rolex rulings”\(^9^1\) in Germany. The courts in these cases ordered eBay and other on-line auction website, to implement measures for prevention of sale of counterfeits on their websites. The courts made significant distinction between the duty to monitor before the infringement has occurred (ex ante) and afterward (ex post), reaching the conclusion that the latter one is

---


\(^9^1\) I ZR 304/01 *Rolex v. Ricardo* [2005] (aka Internetversteigerung I); I ZR 35/04 *Rolex v. eBay* [2007] (aka Internetversteigerung II)
legitimate and can be laid upon ISSPs. Monitoring after the reported infringement concerns monitoring obligation in a specific case.

Besides, Recital 48 ECD declares that the Directive does not prevent Member States from requiring ISSPs “to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities”. Recital 48 ECD prevents ISSPs from being wilfully blind towards illegal content. In other words ISSPs need to be prevented from knowingly avoiding the knowledge of the illegal activity. Although, it is not possible to impose general obligation to monitor, ISSPs cannot ignore the knowledge about illegal content that they have already voluntarily acquired in course of their day-to-day operation.

This interpretation remains plausible also under Czech implementation of the ECD. Section 5 (1) a) of the 2004 Act on ISS provides that the ISSP is only liable if he could have known with regard to the nature of his activity and circumstances and nature of the case, that the content is illegal.\(^\text{92}\) The Czech legal doctrine calls this standard of culpability as “unknown negligence” [nevědomá nedbalost], to distinguish it from the less strict standard of “known negligence” [vědomá nedbalost], where the liable person must have the actual knowledge. Section 5 (1) a) of the 2004 Act on ISS means that in particular case depending among others on the number of occurrences of the illegal content, identity of the content provider, location of the content and on other circumstances, the actual knowledge of the ISSP might not be necessary to hold the ISSP liable, because the ISSP should have known anyway.

So for example, an ISSP is notified about the illegal content. The ISSP removes such illegal content expeditiously, but the same content is uploaded again by the same content provider and even into the very same location. It is more than probable that the hosting ISSP could be held liable for this other occurrences of the illegal content, although he was notified only in respect of originally appeared content that has been duly removed.

Soon there might be more guidance on this question directly from the ECJ, which has already received a reference for a preliminary ruling in L’Oréal v eBay asking whether the ISSP have “actual knowledge” or “awareness” if the illegality is likely to continue to occur through the activity of the same or even different users of the website.\(^\text{93}\)

\(^{92}\) § 5 (1) of the 2004 Act on ISS: “…mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní…”

\(^{93}\) Case C-324/09 Reference for a preliminary ruling from High Court of Justice (England and Wales), Chancery Division, made on 12 August 2009 — L’Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L’Oréal (UK) Limited v eBay International AG,
6. SHIFT TOWARDS MONITORING

The problems with reappearing illegal content, as they were described in the previous chapter, lead us to the Achilles heel of NTD. This weakness stems from the fact that NTD is an ex post solution. Unlike filtering, it cannot prevent the illegal activity from happening in the first place. Moreover, NTD requires aggrieved parties to substantially participate in the elimination of illegal content. Aggrieved parties are forced to bear the costs of fight against illegal activity as they need to monitor the illegal activity and accordingly serve notices in order to eliminate it. This is most noticeable in respect of copyright that is being infringed on a large scale on the internet. Although, one may argue that it is justifiable that aggrieved parties have to pay to enforce their commercial rights such as copyright, this is not applicable to various other illegal activity that damages different than commercial rights and values. Moreover, even in respect of copyright, the participation of aggrieved parties must be limited to reasonable extent.

Described fundamental weaknesses of NTD were aggravated with the rise of Web 2.0 models. New trends in the development of the internet, which took place after the burst of the speculative “dot-com bubble” in March 2000, have brought ever more complex online activity. Although, “father of the internet”, Tim Berners-Lee has contested that popular term Web 2.0 has any distinctive meaning, reminding that the internet was about collaboration of people from its very beginnings, significant changes that have shifted the liability back to online intermediaries were indeed caused by recent development that may be labelled as Web 2.0. Although, it was stated in the very beginning of the final thesis that the NTD seems to be an appropriate measure against illegal UGC, it is not sufficient solution on its own. Following parts will briefly describe the most important trends that have together shifted certain level of liability back to online intermediaries.

6.1. Volume of content

Arguably, the NTD regime would be sufficient solution, if the amount of online information was limited and therefore the aggrieved parties would be able to protect their rights with limited and fair effort. If aggrieved parties have to serve notice only occasionally, the system of NTD could work quiet well.

In the beginnings of the internet only institutions and few technical savvy individuals created online content. However, Web 2.0 brought a user friendly

---

94 eBay Europe SARL, eBay (UK) Limited, Stephan Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi [2009] OJ C267/40, question 9 (c) <http://www.ibm.com/developerworks/podcast/dwi/cm-int082206txt.html> accessed 20 January 2010
environment, which motivates literally every user to become a content provider.\textsuperscript{95} Together with wide expansion of broadband connection and recently higher data rates for wireless mobile phone connection, the amount of user-generated content grew exponentially. Naturally, this growth meant also increase in amount of illegal content.

To secure that NTD serves its purpose, aggrieved parties are forced to bear costs for monitoring online content and report all the infringements to online intermediaries. This approach seems fair, if we realize that aggrieved parties are those who profit from the rights that they are trying to enforce (naturally this reasoning is limited to intellectual property rights). On the other hand, with the growth of illegal content the price for monitoring and notifying is becoming too high. Therefore, it is inevitable that the right holders are trying to shift the costs upon online intermediaries.

6.2. User-generated content as a source of income

Although Web 2.0 services are typically for free, they are indeed generating significant profits.\textsuperscript{96} Profits are created by advertisements that are served alongside UGC. This content is no longer marginal commodity, but it is often the only content provided by the online intermediaries, such as YouTube, eBay or Facebook. UGC has therefore become an essential element of making a profit.

It became more apparent that if intermediaries make profit directly from UGC, they ought to at least partially become responsible for the content. This is most striking in respect of two of the most successful online intermediaries: video sharing website YouTube and online auction and shopping website eBay. Even though YouTube profiles itself as a platform for predominantly amateur and therefore content legally uploaded by its copyright owners, it was well known for hosting large amount of copyright infringing material. Taking into account that YouTube directly profits from every streamed video, it seems more than fair that YouTube was forced to take more active approach in prevention of illegal content. Looking at eBay business model, it can be argued that eBay makes profit from the content even more directly than YouTube. That is because apart from advertising eBay as well charges sellers for concluded transactions (final value fee) and for other services to the sellers (various forms of auction promotion). Some of these auctions concern counterfeits, and eBay consequently directly profits from such illegal activity. Indeed both of these online intermediaries, being forced by manifold law suits, have implemented several proactive measures for prevention of illegal content.

\textsuperscript{95} As Lessig argues in his criticisms of current copyright laws, the 21\textsuperscript{st} century turned to be the ‘read-write’ century in contrast to the ‘read only’ 20\textsuperscript{th} century.

\textsuperscript{96} Naturally, non-profitable sites like Wikipedia are an exception.
6.3. Online intermediaries are no longer endangered species

Another substantial change that took place in the last decade is that online intermediaries have grown stronger. It was almost universally accepted that imposition of more strict liability regimes upon online intermediaries would endanger development of the internet industry as a whole, or alternatively force online intermediaries out of the particular states, which dared to impose more strict liability regimes.\(^{97}\) As a result, the intermediaries would operate from third countries and consequently avoid any compliance with domestic law. Moreover, the activity carried out from third countries would not be properly taxed and states imposing liability on online intermediaries would therefore suffer direct economical loss. This together with already existing safe harbours under the DMCA and CDA in the USA, was also motivation for the European Union to adopt the ECD.

However, today there is no significant concern that more strict liability regimes would endanger development of thriving internet businesses.\(^{98}\) Major online intermediaries hold significant assets in EU Member States. Consequently, the fear, that those online intermediaries would simply leave Member States to avoid more strict liability regime and rather operate illegally from third countries, has diminished.

Stronger position of online intermediaries also enables them to take proactive steps, which reduce illegal activity. For example some news websites in the Czech Republic require prior registration through post.\(^{99}\) In that way, users are de-anonymised and usually do not engage in illegal activity anymore. Of course online intermediaries still have to adhere to NTD procedure, but in case the online intermediary is sued, he will at least have a claim against the particular registered user. Other news websites\(^{100}\) have undertaken more demanding of moderating the discussions.

6.4. Development in technology

With the development of technology, the online intermediaries have gained certain level of knowledge about the UGC and therefore they are slowly loosing the benefits of being mere messengers.\(^{101}\) Not only that the advertisements are attached to

\(^{97}\) This fear partially materialised in Germany. After an unfavourable ruling in ‘CompuServe case’ on 28 May 1998, another online intermediary decided to move the company out of Germany. \(<http://findarticles.com/p/articles/mi_m0UKG/is_208/ai_50276562/> > accessed 23 January 2009

\(^{98}\) L Edwards and C Waelde (eds), Law and the Internet (3rd edn Hart Publishing, Oregon 2009), 85


\(^{100}\) www.aktualne.cz; www.idnes.cz

\(^{101}\) This was as well one of the crucial arguments in notorious French case of LICRA v. Yahoo! The fact that advertisements in French language are being served indicated, that Yahoo! is more or less precisely able to distinguish between the content distributed in France and the content distributed for example in the United States.
the user-generated content, but the advertisements are often targeted. It means that specific advertisements are served to specific users according to their personal profiles. What is significant is that often the advertisements are directly targeted according to the content that is being viewed. This is called contextual targeting. On top of that, there is even more sophisticated advertising method called behavioural targeting. Such targeting principally combines contextual targeting with user profiling. Contextual targeting is characteristic for Google services, but as well for other online intermediaries, such as eBay. Alongside with more precise targeting, online intermediaries as well gain more precise information about nature of user-generated content.

Recently, a lot of attention was given to the development and implementation of “deep packet inspection”. The term describes an activity during which (in our context) online intermediary, which is not a recipient or a sender of information, monitors the very content of the traffic and not only heading information. Deep packet inspection has been severely opposed by human rights watchdogs as too invasive and unlawful practice. It was argued that such practice is in fact interception and therefore must be forbidden. These concerns were particularly strong in connection with advertising system Webwise that was developed, but not yet implemented by American company Phorm. Similar controversy was then sparked by Virgin Media, British online intermediary (access provider), which plans to implement deep packet inspection in order to monitor file sharing. All this may be further developed with ongoing discussion on net neutrality.

Due to the previously presented points and especially due to the development in monitoring technology that enables it, NTD is today supported by many different proactive measures that were implemented by the online intermediaries.

7. CONCLUSION

NTD as a topic of the final thesis was chosen for two major reasons. First, there are many open questions surrounding day to day application of NTD in the Czech Republic. Secondly, as it was illustrated in the last part, liability of online intermediaries

---

102 eBay AdCommerce, see <https://adcommerce.ebaypartnernetwork.com> accessed 24 January 2010
103 See for example <http://news.bbc.co.uk/1/hi/technology/8480699.stm> accessed 10 February 2010
104 For detailed description of the issue see Edwards, L and Waelde, C (eds), Law and the Internet (3rd edn Hart Publishing, Oregon 2009), 531-537
106 For more information start at <http://en.wikipedia.org/wiki/Network_neutrality> accessed 3 December 2010
is very current issue that will inevitably together with NTD undergo further development and therefore deserves to be thoroughly examined.107

First of all, the thesis in its Part 1.2 showed that the 2004 Act on ISS has transposed the ECD in almost verbatim way and thereby the legislator failed to help establish NTD procedures. The significant exception is that the 2004 Act on ISS unlike the ECD actually stipulates liability for the ISSPs that breach NTD.

Chapter 2, looking especially at EU directives, helps set out the scope of the 2004 Act on ISS. It concludes that almost every activity, with exception of search engines, content aggregators and providers of hyperlinks, fall within the scope of the act. However, it also claims that such services need to be protected by the courts following the principle a maiori ad minus. Moreover, it was showed that even entirely free services will benefit from the safe harbours, and that the 2004 Act on ISS applies in respect of civil and also criminal liability.

Chapter 3 explains that although notices under the 2004 Act on ISS may be served by anyone and even anonymously, it is not desirable. An anonymous notice loses its credibility and does not have to inflict the required knowledge of the ISSP about the illegal content. Therefore, such notice could be under particular circumstances found ineffective by the courts. It was also concluded that notice should be served in form of an email and delivered to the address that was made available for that purpose by the ISSP. Otherwise, the ISSP could be able to claim that he did not gain necessary knowledge. At the same time, ISSPs have to make such contact available, if they want to benefit from hosting safe harbour within the 2004 Act on ISS. It was also argued that notice must include identification together with precise location of the content, reason of claimed illegality, and “proof” of illegality of the content where illegality is not self-evident. Moreover notifiers should be aware that they may be found liable for untruthful notice under § 424 of the Civil Code, and ISSPs should limit their liability for take-downs in contractual terms with content providers.

Chapter 4 argues that it should be welcomed that the 2004 Act on ISS did not provide specific time period in which the ISSP needs to act. Instead term “expeditiously” leaves discretion to the courts. The courts will interpret that term based on the qualities of particular ISSP and of reported content.

Chapter 5 addressing the reappearing illegal content reaches conclusion that ISSPs have to be ready to implement certain prevention measures, if they are dealing with repeated infringements.

107 Such suggestion was made, although only in a footnote (no. 13) in Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe COM/2010/0245
It is true that some of the questions that were asked in the final thesis have been already lied down and answered by Polčák\textsuperscript{108} and Říha.\textsuperscript{109} However, the final thesis enabled me to examine these questions in more detail. In addition to that, it may be beneficial that the final thesis was written in English and thereby could enable researches from other Member States easier access and understanding of the Czech regulation.

Some of the more difficult questions could not get direct answers, since the answer will often strongly depend upon facts of the particular case. However, the final thesis, looking at the approaches in other Member States as well as in the United States, has at least outlined the basis for these answers. Moreover, one important point was made in regard of these more difficult questions. ISSPs must realize that they might have to occasionally take more active approach to UGC than the straightforward wording of the 2004 Act on ISS may suggest.

In the last chapter, the final thesis has addressed NTD in more general manner, in order to illuminate that NTD might not be sufficient solution on its own in the near future and that liability of ISSP together with NTD will be inevitably subject to further development.\textsuperscript{110}

\begin{flushleft}

\textsuperscript{109} Říha, J, ‘Odpovědnost providerů se zaměřením na odpovědnost host-providera a access-providera’ 4 Acta Universitatis Carolinae. Iuridica 107

\textsuperscript{110} From all this it is apparent that there is still much uncertainty surrounding the liability of ISSPs. The dominant and the most publicly voiced issue of ISSPs’ liability is undoubtedly the one of copyright infringement. However, it must be pointed out that the roots of this uncertainty in that field do not stem from bad legislation, but from the lack of consensus between stakeholders. The media industry primarily needs to adapt their failing business models and not blindly rely on law enforcement. In other words, it is necessary to adjust the copyright law rather than massively criminalise private individuals or ISSPs. It is necessary that copyright holders themselves revaluate their rights. By making copyright more appropriate for 21\textsuperscript{st} century, the very cause of massive rights infringement will be solved. Media industry must accept that copyright was developed to encourage creativity and not to stifle it in the pursuit of profit.
\end{flushleft}
Bibliography

Books
Reed, C, Internet Law (2nd edn CUP, Cambridge 2004)
Chalmers, D and Davies, G and Monti, G, European Union law: cases and materials (2nd edn CUP, Cambridge 2010)
Lloyd, I, Information Technology Law (5th edn, 2008)
Bainbridge, D, Introduction to information technology law (6th edn Longman, Harlow 2008)
Polčák, R, Právo na internetu - Spam a odpovědnost ISP (Computer Press, 2007)
Steiner, J and Woods, L, EU Law (10th edn OUP, Oxford 2009)

Articles


Herczeg, J and Gřivna, T, ‘Právo na přístup k Internetu, blokace stránek a digitální gigilina’ (2010) 5 Trestněprávní revue 141


Peguera, M, ‘I just know that I (actually) know nothing actual knowledge and other problems in ISP liability case law in Spain’ (2008) 30 E.I.P.R. 280


Robertson, S, ‘Google convictions reveal two flaws in EU law, not just Italian law’ March 2010 <http://www.out-law.com/page-10805> accessed 18 June 2010


Říha, J, ‘Odpovědnost providerů se zaměřením na odpovědnost host-providera a access-providera’ 4 Acta Universitatis Carolinae. Iuridica 107

Smejkal, V, ‘Česká legislativa a informační společnost v roce 2006’ (Systems Integration 2006)


Sensarkar, N, ‘How prepared is the Indian entertainment industry to tackle the challenges posed by Web 2.0?’ 2009


Varas, C, ‘Virtual protection: applying trade mark law within virtual worlds such as Second Life’ (2008)


Wong, H, Ch, ‘eBay's liability for counterfeits: a transatlantic comparison' (2009) 5 JIPLP


‘Google faces Brazil fine for providing forum in which defamation could take place’ (OUT-LAW News, 27 April 2010) < http://www.out-law.com/page-10970> accessed 11 June 2010


# Table of Legal Instruments

**Czech Republic**
Zákon č. 40/1964 Sb., občanský zákoník [Act No. 40/1964 Coll., Civil Code]
Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů [Act No. 480/2004 Coll., on certain information society services and on amendments to certain acts]

**European Union**

**France**
Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [Law for the confidence in the numerical economy]

**Germany**
Gesetz über die Nutzung von Telediensten (Teledienstegesetz – TDG) from 22 July 1997 [Act regulating the use of electronic services]

**Italy**

**United Kingdom**

**United States**
Communications Decency Act of 1996 (CDA)
Digital Millennium Copyright Act 1998 (DMCA)
# Table of Cases

## Australia
*Roadshow Films Pty Ltd & Ors v. iiNet Ltd*[2010] FCA 24

## Czech Republic
*PROLUX Consulting Int., s. r. o. v. Internet Info, s. r. o.* (Municipal court in Prague, 17. 3. 2010, č. j. 10 Cm 47/2009-39)

## Germany
"*CompuServe case*“ (LG München I, 17.11.1999 - 20 Ns 465 Js 173158/95)
I ZR 304/01 *Rolex v. Ricardo* [2005] (aka Internetversteigerung I)
I ZR 35/04 *Rolex v. eBay* [2007] (aka Internetversteigerung II)
I ZR 73/05 *Rolex v. eBay* [2008] (aka Internetversteigerung III)

## Sweden
*"The Pirate Bay"* Stockholm District Court, Division 5, Unit 52, Verdict B 13301-06, (17 April 2009)

## United Kingdom
*L’Oreal SA v eBay International AG* [2009] EWHC 1094 (Ch)

## United States
*ACLU v Reno* 929 F Supp 824 (ED Pa, 1996)
*Zeran v America Online Inc* 129 F 3d 327 (4th Cir, 1997)
*Blumenthal v Drudge and America Online Inc* 992 F Supp 44 (DDC, 1998)
*Tiffany (NJ) Inc. v. eBay Inc.* No 04 Civ. 4607 (RJS) (S.D.N.Y. 2008)
*Perfect 10, Inc. v. Google, Inc.* No. CV 04-9484 AHM (SHx) (26 July 2010)
### Table of Documents


- **Case C-324/09 Reference for a preliminary ruling from High Court of Justice (England and Wales), Chancery Division, made on 12 August 2009 — L’Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L’Oréal (UK) Limited v eBay International AG, eBay Europe SARL, eBay (UK) Limited, Stephan Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi [2009] OJ C267/40**


- **Důvodová zpráva k zákonu č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti) [Explanatory memorandum to the 2004 Act on ISS]**


Czech Abstract


Zákon tak zakotvil do českého právního řádu „Notice and Take Down“. To znamená, že poskytovatel služby, jakmile obdrží oznámení o nelegálním obsahu („notice“), musí neprodleně takový obsah odstranit nebo znepřístupnit („take down“). Neučinil-li tak, vystavuje se sám riziku, že bude za daný obsah odpovídat. Směrnice a ani Zákon však kromě uvedeného pravidla NTD nikterak neupravili. Práce se proto snaží nastínit, jak by měli soudy, ale i poskytovatelé služeb a uživaté postupovat při aplikaci NTD. Aby podkryla smysl ustanovení v Zákoně, práce zkoumá směrnici a její transpozice v některých členských státech. Krom toho se práce rovněž odkazuje na Digital Millennium Copyright Act 1998, který byl hlavní inspirací pro přijetí směrnice.

Na začátku diplomová práce vymezuje působnost Zákona. Dále se věnuje oznámení a konstatuje, že i přesto, že lze oznámení podat anonymně a s minimálním obsahem, je takový postup nežádoucí. Oznamovatel se tak vystavuje nebezpečí, že takové oznámení nezpůsobí prokazatelnou znalost na straně poskytovatele služby a bude tedy neúčinné. Dále práce vysvětluje, že interpretace povinnosti neprodleně učinit veškeré kroky se bude odvíjet jednak od vlastností poskytovatele služeb, tak od kvality konkrétního oznámení, respektive ohlášeného obsahu. Mimo to pak upozorňuje, že poskytovatelé služeb mohou být výjimečně odpovědní i za obsah, který již jednou odstranili, avšak již nepřijali žádná opatření, aby se podobný obsah znovu neobjevoval. V závěru je pak nastiněna širší problematika nelegálního uživatelského obsahu, která spolu s NTD prochází nevyhnutelným vývojem.
Czech Summary

„NOTICE AND TAKE DOWN“, O NĚKTERÝCH ASPEKTECH ODPOVĚNOSTI POSKYTOVATELŮ SLUŽEB

1. Úvod

Diplomová práce se věnuje aktuální problematice z oboru internetového práva. S exponenciálním rozvojem internetu v posledních deseti letech, který je charakteristický takzvaným fenoménem Web 2.0, se jedná o nejdiskutovanějších témat stala odpovědnost poskytovatelů služeb informační společnosti („Information Society Service Providers“) za obsah informací uložených na žádost uživatele („User Generated Content“).

1.1. Odpovědnost poskytovatelů služeb

I přestože problematika odpovědnosti poskytovatelů služeb za uživatelský obsah je značně komplikovaná, ve většině případů v minulosti bylo možné uplatnit prostě pravidlo: poskytovatelé služeb v zásadě neodpovídají za obsah třetích osob, pokud o jeho nelegálnosti nevěděli a ani neměli důvod ji předpokládat. Protože většina poskytovatelů služeb primárně slouží k legálním aktivitám a zpravidla není v jejich silách monitorovat obsah jimi přenášených informací, jeví se tento přístup jako vhodný. Poskytovatelé služeb hrají roli pasivního zprostředkovatele, který stejně tak jako pošta nebo telefonní operátor nezná povahu přenášeného obsahu a nikterak ho ani neovlivňuje. Pokud poskytovatel nemá nad obsahem žádný vliv, pochopitelně za něj nemůže být ani odpovědný.

Na druhou stranu je zde však celá řada praktických důvodů, které podporují snahu dovodit odpovědnost na straně poskytovatelů. Těmito důvody je zejména těžká dosažitelnost uživatelů, kteří zpravidla při šíření nelegálního obsahu vystupují anonymně, případně i dalšími způsoby maskují, odkud nelegální obsah na internet umístuji. Nehledě na to, i pokud je vystopováno koncové zařízení, přes které byl nelegální obsah umístěn, nemusí být zřejmé, kdo dané zařízení k šíření nelegálního obsahu zneužil. Dalším častým důvodem je, že se uživatel nalézá v jiné jurisdikci. To zpravidla značně komplikuje vymáhání práva vůči němu. V neposlední řadě v soukromoprávních sporech hraje významnou roli, pokud uživatel není dostatečně solventní. Oproti tomu je zde zpravidla jasně identifikovatelný poskytovatel služby, který může dokonce sídlit anebo mít pobočky v dané jurisdikci a který má také dostatečné finanční prostředky na to, aby zaplatil případné vzniklé škody a náklady řízení.
Snaha dohnat poskytovatele služeb k odpovědnosti na základě odlišných národních zákonů týkajících se práv duševního vlastnictví, nebo práv souvisejících s pomluvou a jiných, vedla k značné nejistotě na straně poskytovatelů služeb. Jak bude v závěru práce, tato nejistota pak v 21. století dále vzrůstá s rozvojem fenoménu Web 2.0, který představuje internet tvořený především uživatelským obsahem.

1.2. Směrnice o elektronickém obchodu a její transpozice


Každý článek a tedy i jeho ekvivalent v Zákoně zároveň obsahuje podmínky této ochrany před odpovědností. Tyto podmínky v zásadě vyžadují, aby poskytovatel služby nevěděl o nelegálním obsahu, nikterak přenos či ukládání obsahu neovlivňoval a tedy i jakékoliv nakládání s obsahem ze strany poskytovatele bylo zcela automatické. Tyto podmínky by měly zaručit, že se poskytovatel služby vědomě nikterak nepodílel na protiprávních aktivitách uživatelů.

Aby nebyla tato ochrana poskytovatelů členskými státy obcházena, článek 15, který byl transponován § 6 Zákona, zakazuje, aby byl poskytovatel služby nucen přenášený obsah monitorovat. Tak by se totiž poskytovatel služby musel fakticky seznámit s přenášeným obsahem, čímž by ztratil ochranu přiznanou § 3 až 5 Zákona.

1.3. Notice and Take Down

Jedna z podmínek neodpovědnosti poskytovatelů služeb, konkrétně v § 5 Zákona, který upravuje odpovědnost poskytovatele služby za ukládání obsahu informací poskytovaných uživatelem („hosting“), umožňuje vznik takzvané procedury „Notice and Take Down“ (dále jen „NTD“). Podle § 5 odst. 1 písm. b) Zákona totiž poskytovatel služeb odpovídá za obsah informací uložených na žádost uživatele, pouze:
b) dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.

Zákon sice nestanoví jakým způsobem se má poskytovatel o protiprávní povaze uživatelského obsahu dozvědět, avšak vzhledem k tomu, že je (v celku logicky) nutné, aby toto bylo „prokazatelné“, psaně oznámení, tj. „notice“, bude nejčastějším způsobem. Jakmile se poskytovatel o protiprávní povaze dozví, je nutné, aby neprodleně učinil veškeré kroky k odstranění nebo znepřístupnění takových informací, tj. aby provedl „take down“. V opačném případě se poskytovatel služby vystavuje nebezpečí, že bude za daný obsah odpovědný spolu s uživatelem. Paragraf 5 písm. b) Zákona takto tvoří základní stavební kámen pro NTD.


1.4. Cíle a postup diplomové práce

poskytovatel ve vztahu ke znovuobjevujícímu se obsahu. Na závěr se pak práce pokouší zasadit problematiku NTD do širšího kontextu rozvoje odpovědnosti poskytovatelů služeb. Práce se však nezabývá odpovědností jako takovou, ale pouze jejím omezením podle zákona o některých službách informační společnosti.

Základní stavební kámen v podobě § 5 písm. b) Zákona je to jediné co pro konstrukci NTD Zákona stanoví. Přesnou podobu NTD je nutné dovodit zejména pochopením smyslu Směrnice, která v souladu s teorií nepřímého účinku, je cenným zdrojem pro interpretaci Zákona samotného. Diplomová práce se také zabývá některými národními transpozicemi Směrnice a jejích aplikací. Mimo to se práce věnuje ustanovením amerického DMCA, který byl hlavním vzorem pro Směrnici a sám na rozdíl od Směrnice NTD detailně upravil. DMCA i národní transpozice v Členských státech mohou sloužit jako cenná inspirace pro aplikaci NTD v České republice.

2. Působnost


2.1. Poskytovatel služby informační společnosti

Podle § 2 písm. d) Zákona, je poskytovatelem služby každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti. Služba informační společnosti je pak definována § 2 písm. a) Zákona jako:

„jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytnutá zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukladání dat.“

Tato těžko aplikovatelná definice nepřesně opisuje znění obsažené ve Směrnici o postupu při poskytování informací v oblasti technických norem a předpisů 98/34/ES. Daná směrnice však naštěstí byla směrnicí Směrnice 98/48/ES doplněna o přílohu V., která obsahuje výčet služeb, které nelze považovat za služby informační společnosti. Jedná se zejména o služby, které nejsou poskytovány na dálku, protože zákazník je při jejich čerpání například fyzicky přítomen v obchodě poskytovatele. Dále pak služby, které nejsou poskytovány elektrickými prostředky, jako například služby poskytované
přes bankomaty nebo stroje pro automatický výdej parkovacích lístků, ale také například hlasové telefonní služby. A v neposlední řadě pak nelze za služby informační společnosti považovat služby, které jsou *poskytovány současně bez individuální žádosti* neomezenému počtu jednotlivých příjemců, jako jsou zejména televizní a rozhlasové vysílání.

Polčák v souvislosti s kritériem „individuální žádosti“ správně podotýká, že pokud by došlo k důsledné aplikaci definice služeb informační společnosti, přestalo by být zřejmé, kdo je poskytovatelem služby a kdo není. Ve skutečnosti však tyto problémy nevzniknou, protože výše popsané služby, které nejsou službami informační společnosti, mají společnou jednu věc, a to absenci uživatelského obsahu. Tyto služby, tedy nemají důvod hledat ochranu v ustanoveních Zákona.


2.2. **Hosting**

Při určení aplikace NTD pak zejména nesmíme zapomenout, že § 5 Zákona se vztahuje pouze na činnost, která spočívá v ukládání obsahu informací poskytovaných uživatelem, tedy na hosting. Proto Zákon nechráni ani některé poskytovatelé služeb, kteří sice poskytují službu informační společnosti, avšak ne ve formě hostingu. Tyto služby zpravidla nelze zařadit ani do jedné z dalších dvou kategorií, tedy mere conduit podle § 3 a caching podle § 4. Do této kategorie služeb informační společnosti, které nejsou poskytovány ani jednou z chráněných forem, spadají zejména internetové vyhledávače a stránky, které shromažďují obsah z jiných stránek a odkazy. Tito poskytovatelé služeb obsah ani neukládají a ani nevedou nebo dočasně neukládají do vyrovnávací paměti. Místo toho tito poskytovatelé služeb k obsahu pouze odkazují. Tito poskytovatelé se tak nemohou spoléhat na ochranu poskytnutou Zákonem.
Jejich nepostradatelností pro fungování internetu si však byli vědomi již tvůrci DMCA, kteří pro tyto služby vytvořili speciální kategorii „Information Location Tools“. Rovněž pak Španělsko, Portugalsko a Rakousko při implementaci Směrnice zakotvily výslovné ochranu pro tyto služby. V České republice je nezbytné, aby soudy poskytly ochranu těmto službám na základě analogické interpretace § 5 Zákona. Pokud za obsah neodpovídá, ten kdo je ukládá, nemůže logicky za ně odpovídat ani ten kdo k tomuto obsahu pouze odkazuje. To platí samozřejmě pouze za předpokladu, že poskytovatel nemá informace o nelegálnosti takového obsahu.

2.3. Obsah


3. Oznámení

Co se týká oznámení, je potřeba objasnit kdo může oznámení poskytovateli služby podat, jakým způsobem tak může učinit, jaké informace musí oznámení obsahovat a rovněž jak je zabezpečena pravdivost oznámení.

3.1. Kdo může podat oznámení

Protože Zákon nestanoví jinak, lze dovodit, že oznámení může podat kdokoliv. Přestože stejný závěr lze učinit i ve státech jako je Francie, Německo nebo Velká Británie, není taková úprava ideální. Vzniká tak totiž značné nebezpečí zneužití procedury NTD a to jak v rámci hospodářské soutěže, tak v osobních sporech.

Proto například DMCA stanoví, že oznámení může podat pouze poškozená osoba, respektive její zástupce. V režimu DMCA tak oznámení přirozeně musí být opatřeno alespoň elektronickým podpisem. Toto opatření je pochopitelné vezmeme-li v úvahu, že DMCA se vztahuje pouze na práva duševního vlastnictví. O ty by si měl jejich vlastník dbát sám a zpravidla ani nikdo kromě vlastníka nebude mít zájem oznámení podávat. Limitace okruhu oznamovatelů je tak přípustná a přínásí větší
jistotu poskytovatelům služeb. Oproti tomu je však nutné si uvědomit, že Směrnice chrání poskytovatele nejenom proti odpovědnosti za obsah zasahující do soukromých práv, ale i za obsah zasahující do veřejně chráněných zájmů, jako je například obsah podporující terorismu, dětská pornografie a mnoho dalších. Je ve veřejném zájmu, aby na takovýto materiál mohl upozornit kdokoliv. Na druhou stranu jak bude popsáno níže, i přesto, že může v České republice oznámení podat kdokoliv, není v zájmu oznamovalců, jak bude popsáno níže, činit tak anonymně.

3.2. Forma oznámení

Navzdory tomu, že Zákon nestanoví žádné požadavky na formu oznámení, lze dovědět, že oznámení bude vhodné podat písemně. Zákon totiž požaduje, aby se poskytovatel služby o nelegálním obsahu dozvěděl prokazatelně. Je rovněž zřejmé, že preferovaným způsobem je elektronická pošta, která umožňuje snázě lokalizovat závadný obsah. Nehledě na to, článek 5 Směrnice požaduje, aby poskytovatel služby zpřístupnil svůj název, adresu sídla, a emailovou adresu, na které může být rychle a efektivně kontaktovan. I přesto, že daná povinnost nebyla zakotvena v Zákoně, poskytovatelé služby musí nepochybně poskytnout kontaktní údaje. V opačném případě, pokud by nebylo možno poskytovatele služby kontaktovat, nemůže se ani poskytovatel služby spoléhat na imunitu podle Zákona.

3.3. Nezbytné informace v oznámení

Mimo jména a kontaktních údajů stěžovatele, které by v oznámení měli být kvůli věrohodnosti oznámení, oznámení musí bezpodmínečně obsahovat přesnou identifikaci (adresu) závadného obsahu a důvod jeho protiprávnosti. Jako přesnou identifikaci nestačí uvést adresu domovské domény, ale je nutno ji přesně specifikovat. Navíc pokud se jedná například o diskusní vlákno, je vhodné přesně identifikovat, které jednotlivé příspěvky porušují zákon. Poskytovatel služby nemůže být nucen, aby odstranil celé diskusní vlákno z důvodu jednoho či několika protiprávních příspěvků.

V případě obsahu, jehož nelegálnost není patrná bez dalších informací, je nutné rovněž poskytnout i tyto další informace, tedy důvod protiprávnosti. To je typické zejména pokud jde o obsah zasahující do ochrany občanské cti a lidské důstojnosti, či dobré pověsti právnické osoby. V takových případech oznamovalcům musí doložit, že dané informace jsou nepravdivé a jeho čest skutečně poškozují. Pokud tak oznamovalci neúčinní, nelze dovědět, že poskytovatel služby věděl o nelegálním obsahu. Na druhou stranu pokud jde o materiál zjevně nelegální, jako je například dětská pornografie nebo i obsah šířící rasovou nesnášenlivost, kde může být posouzení nelegálnosti obtížnější, je zcela na poskytovateli služby aby dané posouzení provedl. Poskytovatel služby má totiž k posouzení všechny potřebné informace, tedy obsah samotný. Jedná se totiž pouze o posouzení právní otázky, kterou v souladu s
principem *ignoratia legis neminem excusat* poskytovatel služby musí být schopen zodpovědět.

### 3.4. Pravdivost oznámení

Posledním problematickým bodem je právní postavení poskytovatele služby v případě obdržení nepravdivého oznámení. Tento problém lze do určité míry omezit stanovením odpovědnosti oznovatele za nepravdivé oznámení. Tak činí například § 512 (f) DMCA. V České republice může být obdobná odpovědnost dovozena na základě § 424 Občanského zákoníku, který stanoví odpovědnost za škodu způsobenou úmyslným jednáním proti dobrym mravům. Nejmenom, že tato odpovědnost do určité míry odradí osoby od úmyslného podávání nepravdivých oznámení, ale také usnadní poskytovateli služby v dobré víře se spolehnout na pravdivost oznámení, potažmo v dobré víře ohlášený obsah odstranit.


Naší pozornosti by také neměl uniknout § 512 (g) (1) DMCA, který dále posiluje právní jistotu poskytovatelů služeb. Paragraf stanoví, že poskytovatel služby nemůže být odpovědný za odstranění obsahu, které učinil v dobré víře. DMCA tak rovněž chrání poskytovatele služeb před uživatelem, který poskytl legální obsah, a který byl chybným odstraněním takového obsahu poškozen. Obdobnou ochranu český právní řád neposkytuje. Není však vyloučeno, aby si poskytovatel služby vymínil obdobnou imunitu ve smluvních podmínkách s uživatelem. Avšak je nutné upozornit, že takováto podmínka musí být v rozumném rozsahu. Poskytovatel služby v zásadě může odstranit obsah, pouze pokud je v dobré víře, že daný obsah je nelegální. V opačném případě by poskytovatel například mohl zasáhnout do ústavně zaručených práv, jako je svoboda slova a podobně. Ostatně i 46. recitál Směrnice upozorňuje, že při odstranění
obsahu nebo znemožnění přístupu k němu musí poskytovatel služby dodržovat zásadu svobody projevu a s ní spojené postupy stanovené na vnitrostátní úrovni.

4. Povinnost jednat neprodleně

Dozví-li se prokazatelně poskytovatel služby o protiprávní povaze obsahu, nebo o protiprávním jednání uživatele, musí podle § 5 odst. 1 písm. b) Zákona neprodleně učinit veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací. Směrnice, ani Zákon tak přesně neurčili, v jakém časovém horizontu musí poskytovatel služby jednat. Za to si Směrnice respektive její transpozice ve Velké Británii, vysložila kritiku. Ve Velké Británii, totiž rovněž existuje speciální zákon, který omezuje odpovědnost poskytovatelů služeb za obsah podporující terorismus, a který výslovně stanoví dvoudenní lhůtu pro odstranění takového obsahu.


5. Znovuobjevující se nelegální obsah

V souvislosti s NTD rovněž vyvstává otázka, jak je to s nelegálním obsahem, který byl již jednou nahlášen a z internetu stažen, avšak je opět umístěn a to třeba i stejným uživatelem a na stejné místo. Má poskytovatel služby povinnost předejít takovému jednání, respektive takový obsah znepřístupnit i přesto, že nedostal oznámení vztahující se přímo k nově nahranému obsahu?

Vzhledem k tomu, že jak Směrnice, tak Zákon se k problematice opakovaného porušení práv nevyjadřuje, na první pohled se může zdát, že podobná povinnost v České republice neexistuje. Takový závěr však musí být odmítnut. Zejména nelze přehlížet § 5 odst. 1 písm. a) Zákona, který stanoví, že poskytovatel služby je za protiprávní obsah rovněž odpovědný, mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah nebo jednání uživatele jsou protiprávní. Lze dovodit, že touto rozhodující okolností může být právě skutečnost, že
identický obsah nebo obsah od stejného uživatele byl již v minulosti nahlášen a odstraněn.

Je sice pravda, že článek 15 Směrnice, transponovaný § 6 Zákona, výslovně zakazuje, aby byl poskytovatel služby nucen dohlížet na obsah nebo sám aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah, zároveň však Směrnice ve 47. recitálu vysvětluje, že zákaz povinnosti monitorovat se nevztahuje na individuální případy. Například Německé soudy tak v sérii případů internetových dražeb dovodily, že provozovatel internetové dražby měl povinnost učinit opatření, která by omezila opakovaný výskyt nahlášených padělaných výrobků. Soud vysvětlil, že je rozdíl mezi povinností monitorovat internetový obsah ex ante, tedy předtím než došlo k porušení práv, a ex post. Z toho soud vyvodil závěr, že monitorování ex post je přípustné v režimu Směrnice. Takový závěr lze dále také opřít o 48. recitál Směrnice, který stanoví možnost členských států po poskytovatelích služby vyžadovat určitou míru péče v předcházení nelegální činnosti.

Je tedy pravděpodobné, že i soudy v České republice dovodí určité povinnosti poskytovatelů služeb ve vztahu k znovuobjevujícímu se nelegálnímu obsahu. Zejména komerční poskytovatelé služeb budou pravděpodobně nuceni přijmout určitá opatření v případě opakovaného výskytu nelegálního obsahu. Více jistoty v této problematice, by pak v krátké době měl nabídnout i evropský Soudní dvůr, který již obdržel předběžné otázky na toto téma ve věci L’Oréal v eBay.

6. Nárůst monitorování obsahu

Jak vyplývá zejména z předchozí kapitoly, aplikace NTD není zdáleka bez problémů. Hlavní slabinou NTD je jeho ex post povaha. Pomocí NTD nelze trestné činnosti předcházet, ale pouze jí ex post omezovat. S dramatickým rozvojem takzvaného Web 2.0 prostředí v posledních 10 letech, došlo ke zpochybnění základní teze NTD. Jak bude ukázáno, poskytovatelé služeb přestávají být pouhými pasivními zprostředkovateli, kteří nemohou být za uživatelský obsah odpovědní, dokud na ně nejsou prokazatelně upozorněni.

NTD vyžaduje po poškozených stranách, aby na své náklady sledovali obsah internetu a na své náklady rozesílali oznámení. S nástupem fenoménu Web 2.0, který přinesl zejména exponenciální nárůst online obsahu, je taková situace těžko udržitelná. Poškozené strany, zejména mediální průmysl, jehož práva jsou na internetu porušována v největším rozsahu, přirozeně nechtějí tyto vzrůstající náklady nést. Proto se dotčené strany snaží přenést alespoň část těchto nákladů na poskytovatele služeb. Dotčené strany zejména zdůrazňují, že uživatelský obsah včetně toho nelegálního se stal hlavním zdrojem příjmů nejvýznamnějších poskytovatelů služeb. Poskytovatelé služeb totiž v prostředí Web 2.0, veškerý svůj zisk odvozují od reklamy, která je
navázána právě na uživatelský obsah. Díky moderním technologiím, poskytovatelé služeb získávají stále více informací o obsahu, tak aby mohli reklamu efektivně zacílit. Na druhou stranu však poskytovatelé služeb takto ztrácejí postavení pouhých pasivních zprostředkovatelů a nechtěně tak získávají vědomí o nelegálním obsahu. Tím jak se dohled nad obsahem ze strany poskytovatelů služeb stává technicky realizovatelnější, tím je i ospravedlnitelnější.

7. Závěr

Diplomová práce popsala proceduru NTD a objasnila, kterým poskytovatelům služeb takto vznikají povinnosti. Mimo jiné bylo dovozeno, že v České republice může sice oznámení podat kdokoliv, ale neměl by tak činit anonymně. Oznámení je vhodné podat na emailovou adresu, kterou je poskytovatel služby povinen zveřejnit. Oznámení musí zejména obsahovat přesnou adresu nelegálního obsahu a případně důkazy o jeho protiprávnosti. V opačném případě se oznámeovatelem vystavuje nebezpečí, že oznámení nezpůsobí prokazatelnou znalost na straně poskytovatele služby a bude neúčinné. Ten kdo podá nepřesné oznámení, by měl být postihnut podle § 424 Občanského zákoníku. Interpretace povinnosti poskytovatele služby neprodleně učinit veškeré kroky se bude odvíjet jednak od vlastností poskytovatele, tak od kvality konkrétního oznámení, respektive ohlášeného obsahu. Poskytovatel služby by měl rovněž přijmout preventivní opatření v případě znovuobjevujícího se nelegálního obsahu. Mimo to bylo v závěru práce poukázáno na nevyhnutelný vývoj v oblasti odpovědnosti poskytovatelů služeb za obsah informací uložených na žádost uživatele. Práce byla sepsána v anglickém jazyce, a kladě si tak rovněž za cíl pomoci seznámit odbornou veřejnost v členských státech s implementací NTD v České republice.
### List of Keywords

<table>
<thead>
<tr>
<th>English</th>
<th>Czech</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTD</td>
<td>služby informační společnosti</td>
</tr>
<tr>
<td>ISP</td>
<td>směrnice o elektronickém obchodu</td>
</tr>
<tr>
<td>e-Commerce Directive</td>
<td>hosting</td>
</tr>
</tbody>
</table>