The Legal Classification of ISPs

The Czech Perspective

by **Radim Polčák**, Brno
Ph.D, Prof. Head of the Institute of Law and Technology, Masaryk University, Brno

Abstract: This Article is a comprehension of the lecture held at at the International Conference on "Commons, Users, Service Providers – Internet (Self-) Regulation and Copyright" which took place in Hannover, Germany, on 17/18 March 2010 on the occasion of the launch of JIPITEC. It summarizes the current issues concerning ISP liability in the Chzech Republic.

Keywords: ISP liability; Czech Republic; Mere Conduit; Caching Providers; Hosting Providers;

Recommended citation: Radim Polčák, The legal classification of ISPs, 1 (2010) JIPITEC 172, para. 1.

A. Introduction

1 The information society service providers (ISP) represent quite a special group of subjects in the information market. In fact, all activities carried out in information networks happen through these providers. Taking the role of ISPs from the legal point of view, they can be seen as factually contributing to and consequently co-responsible for all kinds of information flow. Finding ISPs as legally co-responsible for illegal activities that take place in the information networks might seem partially unfair – ISPs have neither the technical nor the legal capacity to control the quality of information that is communicated through their services, and so they also have no possibility to prevent their users from illegal acting. On the other hand, if ISPs were totally relieved from their legal responsibilities, there would be no efficient methods for factually enforcing the law. Just as any other activities, law enforcement in information networks is also done through the ISPs; if ISPs were immune from responsibility, law enforcement agencies (police, courts, etc.) would have no means of factually recovering illegal on-line states of affairs.

B. Legislation

2 The Czech legislation that specifically regulates the responsibility of ISPs is based on European Directive No. 31/2000/EC (further referred to in this subchapter as the Directive). The Czech legislator chose to harmonize the rules of the e-commerce directive in the form of a special act. Act No. 480/2004 Sb., on certain services of the information society and on the amendment of corresponding acts, harmonizes not just the regulatory provisions of e-commerce on the responsibility of ISPs but also the prohibitive provisions on spam and some of the administrative competences in the field of e-commerce.

3 The definition of ISP that is used in Act No. 480/2004 Sb. was translated almost word for word from Directive No. 98/34/EC as amended by Directive No. 98/48/EC. Article 2 of Act No. 480/2004 reads as follows:

For the purposes of the present act

(a) information society service shall mean any service provided by electronic means at the individual request of a user submitted by electronic means, normally provided for remuneration; a service shall be

provided by electronic means if it is sent via an electronic communication network and collected by the user from electronic equipment for the storage of data;

(b) electronic mail shall mean a text, voice, sound or image message sent over a public electronic communication network which may be stored in the network or in the user's terminal equipment until it is collected by the user;

(c) electronic means shall mean in particular an electronic communication network, telecommunications terminal equipment and electronic mail;

(d) service provider shall mean any natural or legal person providing an information society service;

(e) user shall mean any natural or legal person who uses an information society service, in particular for the purposes of seeking information or making it accessible;

(f) commercial communication shall mean any form of communication designed to promote, directly or indirectly, the goods, services or image of an enterprise, a natural or legal person who pursues a regulated activity or is an entrepreneur pursuing an activity that is not a regulated activity; also advertising under a special legal regulation shall be deemed to be commercial communication. Data allowing direct access to the activity of a legal or natural person, in particular a domain name or an electronic-mail address shall not be deemed to be commercial communication; further, data relating to the goods, services or image of a natural or legal person or an enterprise acquired in an independent manner by the user shall not be deemed to be commercial communication;

(g) automatic, intermediate and transient storage shall mean storage of information provided by the user that takes place for the sole purpose of carrying out the transmission in an electronic communication network, and the information is not stored for any period longer than is usual in order to carry out the transmission;

(h) automatic, intermediate and temporary storage shall mean storage of information provided by the user that is performed for the sole purpose of making more efficient the information's onward transmission upon request of other users.

4 The criterion "service on individual request" represents in practice an interpretational problem, namely in the case of services that have at once the features of both individually ordered and passively consumed (broadcast) services. As there has been no case law available up until now, it remains disputable whether services such as webcast or various variants of video-on-demand fall under the scope of the legal definition of an ISP. Here we can predict that courts would examine the nature of the respective service and identify the dominant element in the process of ordering and selection of the service content – if the key element is found in active communication, the service will likely be subsumed under the definition of an ISP.

5 Other definitions in Act No. 480/2004 Sb. are with almost no exceptions based on those used in the e-commerce directive. This legislative approach that is based on translations of formulations used in EC directives can also be seen in other parts of harmonized Czech law. In general, we hold the opinion that it might bring a certain level of clarity into the process of harmonization on the one hand, but on the other hand it might cause uncertainties as the translated definitions and other legislative formulations might not always fit properly into the existing system of national law.

6 One of the key questions that arise from the aforementioned legislative approach is whether Act No. 480/2004 Sb. covers only private legal responsibility or whether it also affects the administrative and penal responsibilities of ISPs. Despite the fact that there is missing case law on this question, we firmly hold the opinion that the Act specifically regulates only the private legal responsibility of the ISPs. This interpretation is based on the fact that all the references that are made from Act No. 480/2004 Sb. regarding the responsibility of ISPs are made to the private law legislation (namely to the Civil Code and the Commercial Code). Out of this we might assume that it was not the intention of the lawmaker to link the provisions regarding the responsibility of ISPs to the provisions of administrative or penal law, and consequently that the existing administrative or penal legal responsibility is neither affected nor modified by Act No. 480/2004 Sb.

7 Within the scope of private law, we have to also clarify the question of the applicability of Act No. 480/2004 Sb. in relation to other private legal acts and codes. In particular, there is the question of applicability of the principle lex specialis derogat legi generali when speaking about Act No. 480/2004 Sb. in relation to other private legal legislation. In other words, there is a need to clarify the priority in application of Act No. 480/2004 Sb. As Act No. 480/2004 Sb. applies only on specific subjects of private law – i.e., the ISPs – there is no doubt that its provisions have priority in application over the general foundations of the private legal responsibility laid down in the Civil Code and the Commercial Code. It implies that whenever the foundation of the private responsibility of ISPs is at stake, the limits laid down in Act No. 480/2004 Sb. will apply. Thus, Act No. 480/2004 Sb. is to be understood as special in relation also to the liability grounds laid down in other parts of the private legal legislation. For example, this means that in one of the most frequent cases of illegal activities on line where the Copyright Act applies – copyright infringement – ISPs are also relieved of responsibility to the extent laid down in Act No. 480/2004 Sb.

8 In order to make a distinction between various types of ISPs, Act No. 480/2004 Sb. divides them analog-

ically with the e-commerce directive into three categories:

- Mere conduit providers
- Caching providers
- Hosting providers

I. Mere conduit

9 The definition of mere conduit services including the limits of the liability of their providers is laid down in Article 4 of Act No. 480/2004 Sb. that reads as follows:

> *(1) A provider of a service that consists of the transmission in an electronic communication network of information provided by a user, or the provision of access to electronic communication networks for the purpose of information transmission, shall be liable for the contents of the information transmitted only if he*
>
> *(a) initiates the transmission;*
>
> *(b) selects the user of the information transmitted; or*
>
> *(c) selects or modifies the contents of the information transmitted.*
>
> *(d) The acts of transmission and provision of access under paragraph 1 shall also include automatic, intermediate and transient storage of the information transmitted.*

10 As can be seen from the wording of the above article, the mere conduit providers are defined basically as the providers of the communication links. It should be noted here that the transmission can be provided by both physical and logical means. Therefore, it is not just telecommunication companies or more general providers of connection services (including restaurants with Wi-Fi internet coverage, for example) that fall under the scope of this article, but also the providers of logical services like IP telephony, instant messaging, etc.

11 The liability of mere conduit providers is limited in a relatively broad way, and the only case when the mere conduit ISP might be held liable for illegal content remains the situation when the illegal information is accountable to the respective ISP. Whenever the ISP has not affected the content or the choice of the recipients or has not initiated the transmission of the respective information, there are no grounds for finding it liable for it.

12 There are no provisions in Act No. 480/2004 Sb. that would be parallel to Articles 12(3), 13(2), and 14(3) of the e-commerce directive that give the national legislators an opportunity to legislate takedown or removal duties for ISPs. In this regard it might be considered disputable whether the special provisions of the Czech law under which law enforcement agencies may order mere conduit providers to block the respective service (such as those contained in the Copyright Act) should be held as valid or not. However, the absence of such an express statement in fact does not deprive the legislator from including the takedown duties in specific enforcement provisions as it has to be interpreted in the light of the above-cited provision of the e-commerce directive. Using the argument e silentio legis, we might conclude that the takedown enforcement duties do not fall under the scope of Act No. 480/2004 Sb. and therefore the ISPs are not exempt from any liabilities arising from the takedown enforcement provisions of either the private, administrative, or penal law. In other words, for example, when the Copyright Act lays down the duty to desist with further transmitting of unlicensed copyrighted content, the court might also order the enforcement of this duty against a mere conduit ISP that provides the telecommunication services and is in this case, however, exempt from any other remedies, namely damages.

II. Caching Providers

13 The analogous regime to the case of mere conduit applies to the caching providers. The only difference is in one additional criterion for holding the caching ISP liable for the illegal content of the cached information, i.e., generally speaking, the objective incompliance with the technical or legal requirements for caching. The liability limitation for caching providers is laid down in Article 4 of Act No. 480/2004 Sb. It reads as follows:

> *(1) A provider of a service that consists of the transmission of information provided by a user shall be liable for the contents of automatically, intermediately and temporarily stored information only if he*
>
> *(a) modifies the contents of the information;*
>
> *(b) fails to comply with conditions on access to the information;*
>
> *(c) fails to comply with rules regarding the updating of the information that are generally recognised and used by the industry;*
>
> *(d) interferes with the lawful use of technology, generally recognised and used by industry, to obtain data on the use of the information; or*
>
> *(e) fails to take immediate measures resulting in a removal of or disablement of access to the information he has stored upon obtaining 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 removal of or disablement of access to such information.*

14 The above formulation implies that caching providers might be held liable for the quality of information that is communicated via their infrastructure, not just when the respective information is accoun-

table to them but also when the caching service does not run properly. This might happen in a situation when the source server has already deleted the illegal information but the mirror (or cache) did not react in a proper amount of time, and though the information was already deleted from the source server it still remains in the cache. The technical requirements, however, are considered according to the relatively vague category of industrial practices. This imposes uncertainty on one hand (as of now there is no case law that would clarify the meaning), but on the other hand it enables the courts to adopt and eventually fluently change the practice to correspond to the state of the technology development and the quality and level of development of the local information infrastructure.

III. Hosting

15 From the point of view of ISP responsibility, hosting is the most complex and complicated service of the information society. Here, the ISP provides users with an infrastructure for the storage of their data and eventually makes it available on-line. It is important to note that the law does not make any distinction according to the quality or quantity of the hosted information. Thus, a hosting provider can qualify as such by providing a webhosting service that hosts terabytes of webpages or through a discussion board that in facts hosts only a couple of kilobytes of users' posts.

16 Czech law defines hosting providers and the limits of their private legal responsibilities in Article 5 of Act No. 480/2004 Sb. that reads as follows:

> *(a) A provider of a service that consists of the storage of information provided by a user, shall be responsible for the contents of the information stored at the request of a user only if he*
>
> *(b) could, with regard to the subject of his activity and the circumstances and nature of the case, know that the contents of the information stored or action of the user are illegal; or having, in a provable manner, obtained knowledge of illegal nature of the information stored or illegal action of the user, failed to take, without delay, all measures, that could be required, to remove or disable access to such information.*
>
> *(2) A service provider referred to in paragraph 1 shall always be responsible for the contents of the information stored if he exerts, directly or indirectly, decisive influence on the user's activity.*

17 Czech law uses the concept of unconscious negligence (culpa levis) as the basis for the legal responsibility of hosting providers. It is enough to make the ISP liable, then, to prove that the ISP at least could have known about the illegal nature of the information and did not remove it. There is, however, neither a general monitoring obligation nor an approval for an ISP to monitor the hosted content. Consequently, it is in practice almost impossible to argue unconscious negligence because it would be too difficult to prove that the ISP actually could have known about the illegal information.

18 Thus, the more convenient and practical way of arguing for the liability of hosting providers is through conscious negligence (culpa lata). In this case, the claimant has to prove that the ISP had actual knowledge about the illegality of the stored information. In order to prove that, it is advisable to inform the ISP in a provable way about the fact that some information stored on its infrastructure is illegal. Then, the ISP is given an option either to block or delete the respective information or to be held liable for it.

19 It is to be stressed that the ISP has to be informed in most cases not just about the appearance of the illegal information but also about its illegality. Namely, in cases of defamation or violation of intellectual property rights, there is a need to notify the ISP not just of the fact that the information appeared on its infrastructure, but also of the reasons why the claimant considers the respective information to be illegal.

20 There are neither specific legislative requirements nor any case law regarding the process of the takedown that should be taken by the ISP in order to avoid being responsible for the illegal information. We hold the opinion that Czech courts are likely to follow recent German court practice on this point when the time requirements for a takedown are considered according to the nature of the service and nature of the ISP. The required reaction time will then be differentiated between, for example, the large professional webhosting servers and a private discussion board run as someone's weekend hobby.

21 As can be seen, the law might put ISPs between two kinds of pressure. It can be the pressure of the claimant demanding a takedown of allegedly illegal service on one side and the pressure of the customer with a valid service contract on the other. Moreover, in many cases, it is not prima facie clear whether the respective information is illegal or not. Out of this, certain risks for the ISP might arise:

- If the ISP considers the allegedly illegal data to be appropriate and continues with fulfilling the terms of a service contract (in other words, if the ISP does not take the service down upon notification), the ISP might be held co-responsible if it later turns out in court that the information was illegal.

- If the ISP takes the service hosting the allegedly illegal data down (in other words, if the ISP takes the service down upon notification) and it

later turns out that the data was not illegal, the ISP will be responsible to the client for not fulfilling the terms of the service contract.

22 It is to be noted that any provision of the service contract might not relieve the ISP from responsibility toward third persons – such a liability limitation clause would be completely unenforceable as it is not possible under Czech law to affect the rights of third parties by a mutual agreement. It is also not possible for the ISP to avoid the responsibility by a unilateral disclaimer – if that were attempted, it would not be enforceable. Thus, the only way for the hosting provider to mitigate the risks arising from the responsibility for the user-stored information is:

- the inclusion of a takedown clause in the service contract and/or
- the inclusion of a promise of remuneration of damages in the service contract

23 The takedown must be formulated in a way that would give the ISP the possibility to take the service down only upon the announcement of a third party (the objective illegality would not be required). This would allow the ISP to take down the service upon notification without worrying about being in breach of the service contract if it turns out later that the respective information was not illegal.

24 The promise or remuneration of damages gives the ISP an opportunity to regressively claim the damages that the ISP had to pay to third persons in connection to the hosting service. It does not protect the ISP from responsibility for the users' data, but it gives it a possibility to claim the suffered expenses back afterward.

IV. Monitoring and cooperation

25 In general, ISPs of all types are not required to monitor the information communicated by their clients. This is laid down in Article 6 of the Act No. 480/2004 Sb. that reads as follows:

> *6.) Service providers referred to in Sections 3 to 5 shall not be obliged to*
>
> *(a) monitor the contents of the information which they transmit or store;*
>
> *(b) actively seek facts or circumstances indicating to illegal contents of information.*

26 Moreover, in certain information society services – as in the case of telecommunications or e-mail – the ISPs are even prohibited from monitoring their clients. That makes them not just relieved of the monitoring duty but even legally unable to monitor the quality of communicated information. However, if the ISP reveals for any cause user information that reliably shows that one of the crimes specified below was or is likely to be committed, the person working for the ISP has an immediate duty (just as any other individual under Czech jurisdiction) to announce that fact to the police:

- treason
- subversion of the republic
- terror
- terrorist attack
- sabotage
- espionage
- endangerment of classified information
- infringement of duties relating to manipulation with controlled goods
- infringement of duties relating to international trade with military equipment
- forgery or alteration of money
- infringement of international sanctions
- illegal manipulation with personal data
- participation in criminal conspiracy
- public endangerment
- endangerment of security of an airplane or a ship
- dragging of an airplane to a foreign country
- torture of entrusted person
- murder
- genocide
- use of prohibited measure of warfare

27 Not fulfilling the information duty in the above cases might then lead to criminal prosecution. It is to be noted in this respect that Czech law still does not recognize corporate units as criminally liable, and therefore no fulfillment of the information duty would be recognized as the criminal act of a particular person who learned about the information.

28 As to cooperation duties, the duty to cooperate is formulated in all three types of court procedures – civil, administrative, and criminal litigation – that also apply to all ISPs. According to the respective procedural codes, everyone is obliged to cooperate on the

court procedures in the form requested by the court (in all procedures), state prosecutor (criminal procedures), or police (criminal procedures) without having a right to monetary compensation. Such cooperation might then also include the duty to reveal information or to provide the requested means of evidence (see the subchapter below).

29 The most problematic of the cooperation duties for ISPs is the general duty to cooperate with the police forces that is formulated in Article 47 of Police Act No. 283/1991 Sb. It applies to all subjects under Czech jurisdiction, including ISPs, and reads as follows (informal translation):

(1) *In the course of fulfilling their duties, the police forces are entitled to request help in the form of documents or information from artificial persons, individuals, or state or municipal organs.*

(2) *Organs and subjects named in paragraph 1 are obliged to provide the requested help if it is not contrary to their legal obligations.*

30 The above provisions give the police forces relatively broad competence when speaking about ISPs. As the ISPs are obliged to help the police upon request (without any further specifications), the police might ask them, for example, to block particular communication lines, to take down some webpage, or to provide information about users.

31 There are, of course, legal limits to the above-named competence, namely in the field of privacy and protection of personal data. The extent to which police forces are entitled to use the competence to require the help of ISPs is also limited by general constitutional principles. However, the limits are still relatively broad and allow the police to actively control the flow of information to a relatively large extent.

V. Preliminary and procedural injunctions

32 In general, the procedural law makes a distinction between the preliminary injunctions and various types of procedural injunctions. While the preliminary injunctions are issued in order to preliminarily secure the rights of the parties and/or to make future decisions possible to be issued and enforced, the procedural injunctions are used in order to facilitate the procedure (i.e., to obtain evidence or to enforce the cooperation of various stakeholders). Preliminary injunctions are legislated in Articles 74(1) – 74(3) of the Code of Civil Procedure (Act No. 99/1963 Sb.) that read as follows (informal translation):

(1) *Before the commencement of the proceedings, the chairman of the panel may order a preliminary injunction if it is necessary to regulate provisionally the relationships of the participants or if there is a danger that the enforcement of a judicial decision could be jeopardized.*

(2) *Those who would be participants of the proceedings on the merits shall be the participants of the preliminary proceedings.*

(3) *The competence to order a preliminary injunction shall be exercised by the court that is competent to hear the case unless the law provides otherwise.*

33 The preliminary injunctions can be issued only against subjects with potential passive procedural capacity, i.e., subjects that are potentially legally liable. When Act No. 480/2004 Sb. exempted mere conduit providers from responsibility, it exempted them to the same extent also from the scope of applicability of the preliminary injunctions. Thus, it is not possible to impose a preliminary injunction against an ISP in a situation when the legal exemption in Act No. 480/2004Sb. applies.

34 Procedural injunctions (or procedural orders) do not have that broad material scope of application as preliminary injunctions because they only serve the purpose of fluency of the procedure. On the other hand and unlike the preliminary injunctions, they can be issued against any subject regardless of its recent or potential procedural position. The most important of the procedural injunctions is the injunction on conservation of evidence. It is legislated for the civil procedure in Article 78 of Act No. 99/1963 Sb.) that reads as follows (informal translation):

(1) *Before the commencement of the proceedings on the merits, it shall be possible upon a petition to conserve evidence if there is a danger that the evidence will later not be possible to carry out at all or that it will be possible to carry out only with great difficulties.*

(2) *The conservation of evidence will be carried out by the court that would be competent to hear the merits or by the court in whose district the means of evidence is located.*

(3) *The conservation of evidence shall be carried out by the chairman of the panel in the way prescribed for the concerned evidence. Unless there is a danger of default, the participants of the proceedings on merits shall have the right to be present at the conservation of evidence.*

35 It is to be noted that the above provisions may be used only to the extent that is necessary for the respective procedure. Thus, it is not possible, for example, for a court to confiscate for an unlimited time all the storage facilities of an ISP when just the evidence of storage of some data is to be obtained.