Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Excerpt, pages 163-179

This document is part of the Comparative Study on blocking, filtering and take-down of illegal Internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member States, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

II. METHODOLOGY AND QUESTIONS

1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?

- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet **Access** Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

CZECH REPUBLIC

1. Legal Sources

There is **no specific legislation** on blocking, filtering or take-down of illegal internet content in the Czech Republic. This corresponds to the fact that Czech law does not carry a legal definition of the term blocking, filtering or take-down of illegal internet content. The law in fact provides for freedom of speech and press. An independent press, an effective judiciary, and a functioning democratic political system combine to ensure freedom of expression, including freedom of expression on the internet. However, the law provides for some exceptions to these freedoms, for example, in cases of "hate speech", Holocaust denial, and denial of Communist-era crimes. The law prohibits arbitrary interference with privacy, family, home, or correspondence.

Although there is no specific legislation regarding blocking, filtering or take-down of illegal internet content, there is an **application of the general legislation** on different situations that arose in connection with the operation of the internet. One instance is the Czech Charta of fundamental rights and freedoms that apply to activities on the internet. According to its art. 17 "the **freedom of expression and the right to information** are guaranteed. Everyone has the right to express his views in speech, in writing, in the press, in pictures, or **in any other form**, as well as freely to seek, receive, and disseminate ideas and information irrespective of the frontiers of the state. **Censorship is not permitted**. The freedom of expression and the right to seek and disseminate information may be **limited by law** in the case of measures that are **necessary in a democratic society** for protecting the rights and freedoms of others, the security of the state, public security, public health, or morals".[1] In this sense, there are in the Czech legislation substantive material and procedural safeguards to prevent illegal blocking, filtering or take down of internet content.

Any access to or use of services and applications through electronic communications networks liable **to restrict** the fundamental rights or freedoms may only be imposed if they are appropriate, **proportionate and necessary within a democratic society**, and their implementation is subject to adequate **procedural safeguards**. These safeguards must be in conformity with the European **Convention for the Protection of Human Rights and Fundamental Freedoms** to which the Czech Republic is a contracting party since January 1, 1993. Since the Czech Republic is a member state of the European Union, these safeguards are also in **conformity with general principles of Community law**, including effective judicial protection and due process. A prior fair and impartial procedure is guaranteed.[2]

On August 22, 2013, the Czech Republic ratified the **Convention on Cybercrime** (CETS No. 185) and it entered into force in the Czech Republic on December 1, 2013. The Convention focuses crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.

The Czech Republic on August 7, 2014 also ratified the Additional Protocol to this Convention (CETS No. 189). The Protocol has been in force since December 1, 2014 and entails an extension to cover also **offences of racist or xenophobic propaganda**.

---

1 Charta of fundamental rights and freedoms of 28.12.1992, No. 2/1993 Coll. http://www.psp.cz/cgi-bin/eng/docs/laws/1993/2.html (in English - 29.09.2015).

2 In general Smejkal V. a kolektiv, Právo informačních a telekomunikačních systémů, C.H.Beck, Praha 2001

Further, on July 09, 2001 the Czech Republic ratified the **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (CETS No. 108) (entry into force on 01.11.2001). The Convention protects the individual against abuses which may accompany the collection and processing of personal data and seeks to regulate at the same time the trans frontier flow of personal data. On September 24, 2003, the Czech Republic ratified its Additional protocol regarding supervisory authorities and trans border data flows (entry into force on 1.7.2004).

Moreover, in the Czech Republic the European Union standards apply such as those set out in the Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) or Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the **sexual abuse and sexual exploitation** of children and child pornography.

European Regulatory Framework

In addition, the **European Regulatory Framework** for electronic communications represents a complex of rules to regulate electronic communication networks and services. Five following Directives of the European Parliament and the Council constitute in the Czech Republic fundamental basis of this regulatory framework:

Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (**Framework Directive**),

Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities (**Access Directive**),

Directive 2002/20/EC on the authorisation of electronic communications networks and services (**Authorisation Directive**)

Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (**Universal Service Directive**)

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (**Directive on privacy and electronic communications**).

Transposition of Directives to the Czech national law

Regulatory framework of the European Union was transposed into the Czech legislation mostly by the **Act on Electronic Communications** and on Amendment to Certain Related Acts (the Electronic Communications Act)[3] and by the **Act on certain information society services** and on the amendment to certain other acts (Certain Information Society Services Act[4]). It implements in particular the Directive on electronic commerce, which stresses the duty to safeguard the confidential nature of communications by means of a public communications network and publicly available electronic services.

---

[3] Vaníček Z., Zákon o elektronických komunikačích, Komentář, Linde Praha 2008, Act No. 127/2005 Coll. of 22 February 2005 on Electronic Communications and on Amendment to Certain Related Acts (the Electronic Communications Act), in English: http://www.ctu.eu/164/download/Legal_Regulations/Acts/act_No_127-2005.pdf (29.09.2015).

[4] Zákon o některých službách informační společnosti (http://zakony.centrum.cz/zakon-o-nekterych-sluzbach-informacni-spolecnosti - in Czech - (29.09.2015).

The Act on Certain Information Society Services governs, in accordance with the law of the European Union[5], the liability and rights and obligations of persons providing information society services and disseminating commercial communications. It governs especially **liability of internet service providers**, in particularly liability of the service provider for the contents of the information transmitted, liability of the service provider for the contents of automatically, intermediately, and temporarily stored information and liability of the service provider for the storage of information provided by a user.

Liability of the ISP for internet content

The Act on Certain Information Society Services determines also the extent of the provider's obligations. Service providers **are not obliged to monitor** the contents of the information, which they transmit, or store[6] and they are not obliged to seek facts or circumstances that may indicate illegal contents of information.[7]

A provider of a service that consists of the **transmission of information provided by a user over an electronic communication network**, or the provision of access to electronic communication networks for the purpose of information transmission, is liable for the contents of the information transmitted **only** in the case of following circumstances:

- If he initiates the transmission, selects the user of the information transmitted or if he selects or modifies the contents of the information transmitted.
- The acts of transmission and provision of access include also automatic, intermediate and transient storage of the information transmitted.[8]

A provider of a service that consists of the transmission of information provided by a user is liable for the contents of **automatically, intermediately and temporarily stored information only** if he modifies the contents of the information or fails to comply with conditions on access to the information.[9] He is also liable if he fails to comply with rules regarding the updating of the information that are generally recognised and used by the industry. He is further liable if he interferes with the lawful use of technology, generally recognised and used by industry, to obtain data on the use of the information. He is further also liable if he fails to take immediate measures that the information at the initial source of the transmission has been removed from the network or access to it has been disabled. He is also liable if he fails to take immediate measures to remove or disable access to the information he has stored upon obtaining knowledge of the fact that a court has ordered removal of or disablement of access to such information.[10]

---

5 Mainly Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of information society services, in particular electronic commerce, in the Internal Market and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. The full list of the EU legislation transposed in the Czech legal order, see pages of the Czech telecommunication office (http://www.ctu.cz/predpisy-a-opatreni/pravni-predpisy-eu/smernice-eu.html - 29.09.2015).

6 More detailed information in Polčák R., Právo na internetu, spam a odpovědnost ISP, Computer Press Brno 2007.

7 Act on Certain Information Society Services, Section 6 , „Poskytovatelé služeb … nejsou povinni a) dohlížet na obsah jimi přenášených nebo ukládaných informací, b) aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace."

8 Act on Certain Information Society Services, Section 3.

9 So also in the case on encouraging aggressive war: Muž z Ostravy stanul před soudem, chválil na Facebooku atentát na české vojáky, novinky.cz, 15.06.2015, http://www.novinky.cz/krimi/372350-muz-z-ostravy-stanul-pred-soudem-chvalil-na-facebooku-atentat-na-ceske-vojaky.html (29.09.2015).

10 Act on Certain Information Society Services, Section 4.

A provider of a service that consists of the **storage of information** provided by a user, is responsible for the contents of the information stored at the request of a user **only** if he could know that the contents of the information stored or action of the user are illegal. A service provider is also responsible if he failed to take, immediately, all measures, that could be required, to remove or disable access to information, **which is of illegal nature or based on illegal action of the user**. A service provider is always responsible for the contents of the information stored if he exerts, directly or indirectly, decisive influence on the user's activity.[11]

According to an journalist information, the Czech mobile operators **T-Mobile**[12] and **Vodafone**[13] pass since 2008 mobile and fixed internet traffic through "Cleanfeed", which uses data provided mainly by the **Internet Watch Foundation**[14] to identify pages believed to contain indecent photographs of children, racist materials, extremist and/or terrorist related content, suicide guidelines, anorexia and eating-disorder websites, instructions for weapons construction, drugs consummation, on-line gambling etc.[15]

According to other journalists, **Telefónica O2 Czech Republic**, another Czech DSL incumbent and mobile operator, started in August 2009 without any clear legal sustenance to block access to sites mainly listed by the **Internet Watch Foundation**.[16] It was performed by software that based on pre-set criteria decides whether to prevent the materials from being forwarded. The rollout of the blocking system attracted public attention due **to serious network service difficulties** and many "innocent" sites being mistakenly blocked.[17] The specific blocking implementation is unknown but it is believed that "recursive DNS servers provided by the operator to its customers have been modified to return fake answers diverting consequent TCP connections to an HTTP firewall"[18].

In May 2010, T-Mobile Czech Republic officially announced that it was starting to block web pages promoting child pornography, child prostitution, child trafficking, pedophilia and illegal sexual contact with children. T-Mobile claimed that its blocking was based on URLs from the Internet Watch Foundation list and on individual direct requests made by customers. According to the newspaper information, in October 2011, a petition was submitted protesting the effort to restrict foreign online gambling and **demanding a law guaranteeing censorship free access to the internet and browsing.**[19]

---

11 Act on Certain Information Society Services, Section 5.

12 Peterka J.,*T*-Mobile jde do UMTS FDD a do blokování nelegálního obsahu (T-Mobile goes into UMTS FDD and blocking of illegal content), , Lupa.cz, 16 December 2008, http: //www.lupa.cz/clanky/t-mobile-jde-do-umts-fdd/ (29.09.2015).

13 Peterka J., Stalo se: je cenzura Internetu už i v ČR?, Lupa.cz, 30 June 2008, http://www.lupa.cz/clanky/stalo-se-je-cenzura-internetu-uz-i-vnbspcr/ (29.09.2015).

14 Internet Watch Foundation, https://www.iwf.org.uk/.

15 Rylich J., Regulace jako budoucnost Internetu?, 27. June. 2008, http://www.lupa.cz/clanky/regulace-jako-budoucnost-internetu/ (29.09.2015).

16 T-Mobile pomáhá v boji proti zneužívání dětí blokováním nelegálního obsahu. (T-Mobile helps in the fight against the abuse of children by blocking illegal content), press release, T-Mobile.cz, 6 May 2010, (no more accesible). Although the company said it wanted to replace the list with data provided by Czech Police, it never published or made accessible the lists of blocked or filtered sites.

17 Macich J. ml, Klienti Telefóniky O2 si stěžují na blokování webů, Lupa.cz, 13 August 2009, http://www.lupa.cz/clanky/klienti-telefoniky-o2-si-stezuji-na-blokovani-webu/ (29.09.2015).

18 Jiří Peterka J., Stalo se: Už i Telefónica přistoupila k blokování, , Lupa.cz, 17 August 2009 http://www.lupa.cz/clanky/stalo-se-uz-i-telefonica-blokuje/ (29.09.2015) et http://www.lupa.cz/clanky/telefonica-o2-potvrdila-filtrovani-stranek/ (29.09.2015).

19 Prague Daily Monitor (Czech News Agency), 26 October 2011. Pirate Party succeeds with petition against Internet censorship.

The main criticism of blocking internet content by private entity (IPS) is based on the fact that such conduct is made "voluntarily" without any legal bases and **outside the legal framework** as well as without any distinction between law-based and non-law based action. Access to selected websites in above mentioned cases was not based on law, but on decisions by private-law entities (ISPs). The criteria for blocking were in consequence not clear, blocked websites were not listed and above **all appeal processes were extremely onerous or effectively impossible**. The state authorities do not in any event encourage private actors to block voluntarily or to censor internet content themselves. According to the Act on electronic communication if the service could be used only partially, or could not be used at all, because of a technical or operating fault on the side of the undertaking that provides the service, such an undertaking must ensure that the fault is removed. In this case the price must be adequately reduced, or the ISP may agree with the subscriber that the service will be provided in a substitute manner.[20] Despite all the criticism against censorship decisions made without public discussion by private entities and without an appeals process, it is unquestionable that there is certain content that is a legitimate target for blocking measures, which **can be based only on the decision of the court**. It is also accepted if the ISP provides possibility of internet content blocking on demand or based on the contract with end-users (parental protection choice).[21] Actually, in absence of pending court cases, ISPs do not report voluntary measures to block internet content.

The main source of the Czech law

The main source of the Czech law is a written legislation. Its main areas are systematically codified, mainly in Civil Code and Criminal Code. The form of court proceeding including safeguards against illegal procedure is prescribed in the Codes of Criminal, Civil and Administrative Procedure. The Czech legislation applicable on blocking, filtering and take down of illegal internet content includes mainly the following laws:

Charta of fundamental rights and freedoms of 28.December 1992 (No. 271993 Coll.)[22]

Penal Code of 8 January 2009 (No. 40/2009 Coll.)[23]

Code on Criminal Procedure of 29 November 1961 (No. 141/1961 Coll.)[24]

Civil Code of 3 February 2012 (No. 89/2012 Coll.)[25]

Civil Procedure Code of 4 December 1963 (No. 99/1963 Coll.)[26]

Act on **Certain Services of the Information Society** (No 480/2004 Coll.)[27]

---

20 Act on electronic communication Art 64 para 12, "Pokud službu bylo možno využít jen částečně, anebo ji nebylo možno využít vůbec pro závadu technického nebo provozního charakteru na straně podnikatele poskytujícího službu, je tento povinen zajistit odstranění závady a přiměřeně snížit cenu nebo po dohodě s účastníkem, který je koncovým uživatelem, zajistit poskytnutí služby náhradním způsobem. Podnikatel poskytující službu elektronických komunikací není povinen nahradit jejím uživatelům škodu, která jim vznikne v důsledku přerušení služby nebo vadného poskytnutí služby."

21 Šlemarová D., Cenzura internetu – krutá realita?, itpravo.cz 23.06.2010, http://diit.cz/clanek/cenzura-internetu-kruta-realita (29.09.2015).

22 See note Nr. 1.

23 Trestní zákoník č. 40/2009 Sb., (http://zakony.centrum.cz/trestni-zakonik - in Czech - 29.09.2015).

24 Zákon o trestním řízení soudním (trestní řád) č. 141/1961 Sb. (http://www.zakonyprolidi.cz/cs/1961-141 - in Czech - 29.09.2015).

25 Občanský zákoník č. 89/2012 Sb., (http://obcanskyzakonik.justice.cz/fileadmin/NOZ_interaktiv.pdf - in Czech - 29.09.2015).

26 Občanský soudní řád č. 99/1963 Sb. (http://www.zakonyprolidi.cz/cs/1963-99 in Czech - 29.09.2015).

Act on **free access to information** (No. 106/1999 Coll.)[28]

Act on **Electronic Communications** and on Amendment to Certain Related Acts (Electronic Communications Act) (No. 127/2005 Coll.)[29]

Act on the **Cyber Security** and on the Amendments of the Related Acts (Cyber Security Law) (No. 181/2014 Coll.) [30]

2. Legal Framework

Measures taken by authorities of the Czech Republic regarding blocking, filtering and take-down of content on electronic communications networks **respect the fundamental rights and freedoms** of natural and legal persons. Any of these measures may only be imposed if they are **appropriate, proportionate and necessary** within a democratic society, and their implementation is subject to adequate **procedural safeguards**. Content of the internet is judged by court like documentary paper evidence.

2.1. Blocking and/or filtering of illegal Internet content

2.1.1. Criminal Law Provisions

Under the **Czech Penal Code** in general the principle that applies is: "what is illegal off-line is also illegal on-line".[31]

Following conducts are illegal under the Czech Penal Code (in order in which they appear in the Penal Code):

Use of Personal Data[32] - Whoever, even out of negligence, publishes, discloses, makes available, or otherwise processes or appropriates personal data that was collected on another person in connection with the execution of public authority without authorisation, and thus causes serious harm to the rights or legitimate interests of the person whom the personal data concerns is liable. An analogous crime holds liable whoever, even out of negligence, violates the State imposed or recognised obligation of confidentiality by publishing, disclosing, making available, or otherwise processing or appropriating personal data that was collected on another person in connection with the execution of their employment, profession, or function without authorisation, and thus causes serious harm to the rights or legitimate interests of the person whom the personal data concerns.

---

27 Zákon o některých službách informační společnosti (http://zakony.centrum.cz/zakon-o-nekterych-sluzbach-informacni-spolecnosti - in Czech - 29.09.2015).

28 Zákon č. 106/1999 Sb. ze dne 11. května 1999 o svobodném přístupu k informacím, https://portal.gov.cz/app/zakony/download?idBiblio=47807&nr=106~2F1999~20Sb.&ft=pdf (29.09.2015).

29 Zákon ze dne 22.02.2005 o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) č. 127/2005 Sb. http://www.zakonyprolidi.cz/cs/2005-127 (29.09.2015).

30 Zákon ze dne 23. 07. 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) č. 181/2014 Sb., http://www.nbu.cz/cs/pravni-predpisy/zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/ (29.09.2015).

31 See Kybernetická kriminalita, Iuridica 4/2012, Acta Universitatis Carolinae, Praha 2013.

32 Penal Code Section 180.

Infringement of Stranger's Rights[33] **-** causing serious harm to the rights of someone else by bringing another person into error.

Slander[34] - bearing a false statement about another person that is capable of substantially jeopardising their esteem among their fellow citizens, especially in their employment, disruption to their family, or to cause them any serious damage.

Distribution of Pornography[35] – holds liable any person that produces, imports, exports, transports, offers, makes publicly available, provides, puts into circulation, sells or otherwise procures photographic, film, computer, electronic or other pornographic works that reflect violence and disrespect to human beings or that describes or depicts or otherwise displays sexual intercourse with an animal.

Production and other Handling of Child Pornography[36] – holds liable a person who possesses photographic, film, computer, electronic or other pornographic works which display or otherwise use a child. The same crime commits whoever produces, imports, exports, transports, offers, makes publicly available, provides, puts into circulation, sells or otherwise procures photographic, film, computer, electronic or other pornographic works that display or otherwise use a child or who exploits such pornographic works.

Endangering a Child's Care[37] – holds liable anyone who, even out of negligence, endangers the intellectual, emotional, or moral development of a child by enticing it to an indolent or immoral life, allowing it to lead an indolent or immoral life, or allowing them to procure means for themselves or others through criminal activity or by another condemnable manner. A same crime commits whoever allows, even out of negligence, the child to play on slot machines equipped with a technical device affecting the outcome of the game and which provides the possibility of monetary winnings.

Unauthorised Access to Computer Systems and Information Media[38] -- holds liable any person who overcomes security measures and thus gains access to a computer system or part thereof without authorisation. Any person who gains access to a computer system or information medium and uses data stored in a computer system or information media without authorisation, who erases or otherwise destroys, damages, amends, suppresses, or corrupts the quality of data stored in a computer system or information media, or renders them unusable without authorisation, or who forges or alters data stored on a computer system or information media so as to be considered authentic, and according to them was treated as if it was authentic data, notwithstanding the fact whether the data is directly readable and understandable, or who inserts data into a computer system or information media or performs any other intervention into the software or hardware of the computer or other technical data processing equipment without authorisation commits the same crime.

A crime of **Measures and Possession of Access Devices and Computer System Passwords and other such Data** holds liable a person who intends to make a criminal offence of violating confidentiality of messages or a criminal offence of unauthorised access to computer systems. The same crime makes liable a person who puts into circulation, imports, exports, transports, and offers, provides, sells, or otherwise makes available, instrument or any other means, including a computer programme,

---

33 Penal Code Section 181.
34 Penal Code Section 184.
35 Penal Code Section 191.
36 Penal Code Section 192.
37 Penal Code Section 201.
38 Penal Code Section 230.

designed or adapted for unauthorised access to electronic communications networks, a computer system or part thereof. The same crime makes liable a person for the same unauthorised activity with a computer password, access code, data, process or any other similar means with which they are able to gain access to a computer system or part thereof.[39]

Violation of Copyright, Rights Related to Copyright and Database Rights[40] holds liable anyone whointerferes, substantially, with the legally protected rights to authorship works, artistic performance, audio or audio-visual recordings, radio or television broadcasts, or a database without authorisation.

Distribution of Drug Addiction[41] holds liable anyone whoentices another person to the abuse of addictive substances other than alcohol or supports them in it, or whoever otherwise encourages the abuse of such substances or distributes them.

Dangerous Persecution[42] holds liable anyone whopersecutes another person long term by threatening him/her with bodily harm or a person close to that person, seeking out their personal closeness or watching them, persistently contacting them via means of electronic communications, written or otherwise, restricting them in their usual way of life, or abusing their personal data in order to obtain personal or other contact, and such conduct is capable of raising substantial concerns in them for their life or health or the life or health of persons close to them.

Defamation of Nation, Race, Ethnic or other Groups of People[43] holds liable anyone whopublicly defames any nation, its language, any race or ethnic group, or any group of people for their actual or perceived race, ethnicity, nationality, political, belief, religion, or because they are actually or allegedly non-religious.

Encouragement to Hatred against a Group of People or to restrict their Rights and Freedoms[44] holds liable anyone whopublicly encourages the hatred of any nation, race, ethnicity, religion, class or another group of people, or to restrict the rights and freedoms of their members.

Spreading of Alarming News[45] holds liable anyone whointentionally causes the risk of serious concern of at least part of the population of a certain place by spreading alarming news that is false. Whoever communicates the false news that is capable of causing measures leading to the risk of serious concern of at least part of the population of any place, or the undue rescue work of the Integrated Rescue System to the courts, police authority of the Police of the Czech Republic, public authority, local government or another public authority, a legal entity, natural person who is an entrepreneur, or a means of mass information commits the same crime.

A crime of **Encouragement of a Criminal Offence**[46] holds liable anyone whopublicly encourages a criminal offence.

An **Approval of a Criminal Offence**[47] holds liable anyone who publicly approves of the committed

---

39 Penal Code Section 231.
40 Penal Code Section 270.
41 Penal Code Section 287.
42 Penal Code Section 354.
43 Penal Code Section 355.
44 Penal Code Section 356.
45 Penal Code Section 357.
46 Penal Code Section 364.
47 Penal Code Section 365.

crime or whoever publicly extols the offender for the crime.
A crime of **Expressions of Sympathy for Movements Seeking to Suppress Human Rights and Freedoms**[48] holds liable anyone who publicly expresses sympathy for the movements seeking to suppress Human Rights and Freedoms.

A **Denial, Questioning, Approval and Justification of Genocide**[49] holds liable anyone who publicly denies, questions, approves, or attempts to justify Nazi, Communist or any other genocide, or other crimes of the Nazis and Communists against humanity.

A crime of **Encouraging Aggressive War**[50] holds liable anyone who publicly encourages an aggressive war, in which the Czech Republic is to participate, promotes such a war, or otherwise supports the war propaganda.

As an integral part of the court decision that finds that a crime has been committed on the internet, the **court may also order a ban on the continuation of the crime**. This happens by way of an order to internet service providers to **block or remove the illegal content**. Although there are no criminal cases that explicitly apply to blocking or removing of internet content, this possibility legally exists. In addition, this procedure can be done according to the Czech Code of Criminal Procedure[51] more effectively in the framework of interim measures, i.e. before final court decision (see below). There is no information how it works in practice, because corresponding decisions on removal or take down of illegal internet content are not available.[52] We assume it will have the same procedure as when the court orders a ban on continuation of the crime in a non- internet matters. After the decision of the court and after delivery of the court decision to the ISP, the ISP must remove the illegal content.

2.1.2. Civil Law Provisions

In some cases the content of the internet does not constitute a criminal offence, although it has some wrongful aspects. In such cases it is possible to use a civil legislation to block or take down internet content. It relates currently in the Czech Republic e.g. to internet cases concerning defamation of certain groups of persons in relation to migration[53] or to a website of the Czechoslovak paedophilia community[54]

Such considerations are based on the fact that under the Czech Civil legislation, **everybody was obliged** to behave in such a way that **no damage** to health, property, nature and living environment occured.[55] Such behaviour, also when it is committed through the internet, may be challenged by a legal action and connected also with request to block or take down internet content. Any person may

---

48 Penal Code Section 404.

49 Penal Code Section 405.

50 Penal Code Section 407.

51 Code of Criminal Procedure Section 88b, 88c and 88l. An imposed measure is “a prohibition of particular defined activities”.

52 In fact the questionable content disappears from the net before possible order of the court.

53 http://www.novinky.cz/domaci/380038-za-sireni-nenavisti-na-internetu-padlo-uz-70-oznameni.html (29.09.2015)

54 According to investigations of Czech police website of Czechoslovak paedophilia community (http://www.pedofilie-info.cz/cepek-ceskoslovenska-pedofilni-komunita/) is not illegal, does not contradict the criminal law and only private action can be raised, e.g. against portraits or published photographs of children. This exposure can be challenged by children itself or by their parents. See: Web pedofilie-info podle policie zákonu neodporuje, 04.08.2015 http://www.novinky.cz/krimi/376698-web-pedofilie-info-podle-policie-zakonu-neodporuje.html (29.09.2015)

55 Civil Code Section 2900.

request the court to protect the private right, which has been threatened or violated on the internet (e.g. by dissemination of photographs of children on the home page of the Czechoslovak paedophilia community). Part of such a claim may also be a request for termination of such conduct. The decision of the court in the civil procedure may involve blocking or take down. In civil law too, the general principle that "what is illegal (prohibited) off-line is also illegal (prohibited) on-line" applies. In civil judicial proceedings, courts hear and decide disputes and other legal matters and carry out enforcement in case there is no voluntary execution of the judgment. In exercising their function, courts ensure also within internet activities that there is no violation of the rights and interests protected by civil law and that the rights are not abused.[56]

Also any person is, according to the Czech civil legislation, liable through his or her activity on the internet for damage which he/she causes by breaching his/her legal duty.[57] The competent authority on liability issues is **the court**. The court decides in the **final judgment or, at an earlier stage, in preliminary ruling**[58] to provisionally modify the relation of participants (including blocking or take down of internet content).

In addition, **papers of a personal nature**, portraits, pictures, and video and audio (sound) recordings concerning a certain individual or expressions of a personal character may be **used only with his consent**. Such consent is not required if papers of a personal nature, portraits, pictures, or video and audio (sound) recordings are used for official purposes on the basis of law. Portraits, pictures, visual and audio (sound) recordings may also be used without the consent of the individual in an appropriate manner for scientific or artistic purposes, as well as for purposes of news reporting by the press, film, radio and television. However, such use may not conflict with the warranted interests of the individual concerned.[59]

An individual has a particular right to **demand that there be no unjustified interference in his right** of personhood, **that the consequences of such interference be eliminated** and that appropriate satisfaction be rendered, including through **removal or blocking[60] of the illegal internet content**.[61] Should this satisfaction not prove sufficient, in particular due to the fact that the individual's dignity or reputation in society was diminished to a significant extent, the individual concerned also has the right to **monetary compensation** of such non-proprietary detriment.[62] The court determines the amount of

compensation, taking into account the seriousness of the detriment suffered and the circumstances under which the violation of the right took place.[63]

---

56 Antoš M., Kauza Prolux - rozsudek odvolacího soudu, http://blog.lupa.cz/man/kauza-prolux-rozsudek-odvolaciho-soudu/(29.09.2015); Decision of the Supreme Court of 2 march 2011 http://i.iinfo.cz/files/lupa/551/prolux-vs-mesec-rozsudek-vrchniho-soudu.pdf (29.09.2015) and idnes Zpravy 17. March 2010: http://zpravy.idnes.cz/soud-vytahl-bic-na-internetove-diskuse-kritizujte-ale-nenadavejte-1dp-/krimi.aspx?c=A100317_164353_krimi_abr (29.09.2015) and idnes Zpravy 4. Mars 2011: Diskuse naštvaných klientů se mazat nemusí, je to svoboda projevu, Zdroj: http://zpravy.idnes.cz/diskuse-pod-clankem-v-niz-klienti-kritizuji-firmu-se-nemusi-smazat-rozhodl-soud-gfj-/domaci.aspx?c=A110304_120015_krimi_wlk (29.09.2015).

57 Civil Code Section 2894.

58 Code of Civil Procedure Section 74.

59 Civil Code Sections 84 – 89.

60 Until now no such cases are reported.

61 Civil Code Sections 78 and 2956.

62 Civil Code Sections 82 and 2951.

63 Civil Code Section 2957.

Compensation is provided for actual damage, and for profit lost by the injured party.[64]

2.1.3. Administrative review

No administrative authority can on its own forcefully order blocking, filtering of the content from electronic communications networks. There is **no administrative restriction** on access to the internet or credible reports that the administrative authority monitors content of internet, e-mail or internet chat rooms without judicial oversight.

2.2. Take off down/removal of illegal internet content

The Czech **legislation does not define** blocking, filtering or taking down and removal of illegal internet content and therefore also does not distinguish between these concepts. The above information related to blocking and filtering of illegal internet content can be considered valid also for take-down or removal of such content. According to the Czech legal order only Court decisions may establish legal grounds for take-down, removal or blocking of internet content.

1. Procedural Aspects

There are in the Czech legislation substantive material and procedural safeguards to prevent illegal blocking, filtering or take down of internet content. Any access to or use of services and applications through electronic communications networks liable **to restrict** the fundamental rights or freedoms may only be imposed if they are appropriate, **proportionate and necessary within a democratic society**, and their implementation is subject to adequate **procedural safeguards**. These safeguards must be in conformity with the European **Convention for the Protection of Human Rights and Fundamental Freedoms** to which the Czech Republic is a contracting party. Thus all restrictions are based on law and on procedural safeguards which are laid down in the Czech Criminal and Civil Procedures. The judicial review procedures concerning the blocking of internet sites meet the general criteria for avoiding abuse. The Czech legal order ensures that restrictions on access to internet content are based on a strict and predictable legal framework which also guarantees a judicial oversight of these restrictions.

Although the use of procedural rules for blocking and take –down of the internet content are not yet found in the Czech Republic, it is important that there are applicable rules which enable the Czech courts to exam necessity of blocking measures, their effectiveness and adequacy and which allow the courts to resolve all conflicts in view of the particular circumstances of each case. That is why we mention hereinafter procedural rules of criminal and civil proceedings.

3.1. Criminal Procedure

For criminal procedure, the chief statutory regulation is Act No. 141/1961 Coll., the Code of Criminal Procedure. Enforcement of the decision to block, filter or take down content of the internet follows by the way of **enforcement of the court decision** foreseen by the Law. An **interim measure**, including measures consisting of blocking internet content, may also be ordered by the presiding judge at the initiation of the proceedings , if necessary, to prevent the continuation of crime.[65]

---

64 Civil Code Section 2894.

65 Code of Criminal Procedure Section 88l. The Act No. 480/2004 Coll. on certain services of the information society Art. 5 makes hosting providers responsible for failing to block or remove illegal content it was made aware of.

The **Police** authority is obligated by the Code of Criminal Procedure[66], to take all necessary measures to uncover a criminal offence. This can be done based on their own findings, criminal reports, and instigations by other persons and authorities because of which conclusions may be made on the suspicion of a criminal offence. The police is further obliged by law in identifying the offender and whenever possible, to take the **necessary measures to prevent the criminal activity**. According to news reports the Czech police is using RCS monitoring software developed by the Hacking team company. The police confirmed that it uses monitoring software in accordance with the law. All other information is treated by the police as confidential and will not be released.[67]

The Public Prosecutor and the police authority are required to accept reports of facts suggesting that the criminal offence was committed. At the same time, they are obligated to instruct the reporting person about the liability incurred for making knowingly false statements and if the reporting person requests it, to inform them on the effective measures taken within one month of the notification.

The Police authority creates a record to clarify and verify the **facts reasonably suggesting that a criminal offence was committed**, stating the facts based on which the proceeding is being commenced, and how they learned about them. They send a copy of the record to the Public Prosecutor within 48 hours after the initiation of the criminal proceedings. If there is a **danger of delay**, the Police authority makes a record after completing the **necessary urgent or non-reproducible tasks**.

The Police **authority secures the necessary evidence and necessary explanations, and traces of the criminal offence to clarify and verify the facts** reasonably suggesting that a criminal offence was committed. As part of it and in addition to other actions, they are also in particular entitled to **require an explanation or cooperation from natural persons and legal entities and public authorities**, to require professional statements from the competent authorities and, if it is necessary for the assessment of the matter, also expert opinions, to **secure the necessary documents**, in particular the writings and other written materials, and to conduct an examination of the items and crime scene.

3.2. Civil procedure

Code of Civil Procedure governs the procedure of the court and the parties in civil proceedings so as to ensure **fair protection of private rights** and legitimate interests of the participants, as well as to ensure honest performance of duties and to respect the rights of others. For these purposes, the presiding judge may order **an interim measure**[68] (including blocking and take down of internet content) before proceedings are initiated. These measures are ordered if necessary to provisionally modify the relation of participants, or if it is feared that the enforcement of the judicial decision could be jeopardised in the civil procedure. The participants in the civil proceedings include the plaintiff and those who would be participants if the matter itself was concerned.

To cover any **compensation for damage** or any other loss that would be caused by the interim

---

66 Code of Criminal Procedure Section 158.

67 Policie ČR: Šmírovací software jsme koupili, ale vše je tajné, nic neřekneme, Lupa. Cz 7.7.2015 http://www.lupa.cz/clanky/policie-cr-smirovaci-software-jsme-koupili-ale-vse-je-tajne-nic-nerekneme/ (29.09.2015), Hackeři podlehli útoku, unikly faktury a hesla. Kupovala i Policie ČR, Technet.cz 7.7. 2015 http://technet.idnes.cz/hacking-team-hacknut-unik-0hh-/sw_internet.aspx?c=A150707_175012_sw_internet_pka#utm_source=sph.idnes&utm_medium=richtext&utm_content=clanek-box (29.09.2015).

68 Code of Civil Procedure Section 75.

measure, the plaintiff shall be obliged to give **security** amounting to CZK 10000 and CZK 50,000 in business matters no later than on the day when the plaintiff filed the interim measure proposal at the court. If the presiding judge concludes that the security paid is evidently insufficient to provide compensation for the damage or any other loss that would be caused by the interim measure, he or she will, without undue delay, call upon the plaintiff to pay within 3 days a supplement on security in an amount that he or she determines after considering the case circumstances. If **more plaintiffs** have filed an interim measure proposal, they will be obliged to give security jointly and severally. If security is not given, the presiding judge will refuse the interim measure proposal. This will not be the case if there is a risk of delay. The consequence of delay could include loss upon the plaintiff and the plaintiff testifying that he could not give security without fault on the part of the plaintiff.

If the interim measure ordering proposal has been refused by a final resolution of a court of the first instance or if such proposal has been finally refused, or if proceedings for such proposal have finally been stopped, the court returns the paid security. If the court has ordered an interim measure, the **security will be returned if a court decision on an action filed is in full force** and effect and the decision suggests that the **security will not be used to satisfy** the right to indemnity or any other loss.[69]

An interim measure may especially impose on the participant e.g. the obligations not to dispose some items or rights or to perform something, refrain from something, or permit something. E.g., project Chocen.TV[70] ended camera operation because after years of operation the Czech Railways stated, that the transmission of online information on websites and mobile applications represents an increased security threat to rail traffic. The operator of the camera immediately stoppedthe transmission via internet , even before interim measure of the court (but continues in an authorized recording of rail traffic off-line).[71]

An interim measure, including. measures consisting of blocking internet content, may **impose an obligation on a person other than the participant** of the hearing if this may justifiably be requested from such person.[72] When an interim measure is ordered, the presiding judge generally requires the plaintiff to file a proceedings initiation proposal at the court in a time specified by the court, except if proceedings for the matter may be initiated without any proposal. The presiding judge may also provide that the interim measure only lasts for a specified time.

If required by the case circumstances or a risk of delay is being faced, the presiding judge will without undue delay, **immediately declare the interim measure resolution**, on which it has decided, to take effect on the **participant on whom an obligation is imposed or any person other than the participant** in the proceedings if an obligation has been imposed by the interim measure on such person; if proving to be necessary, the presiding judge will pronounce the resolution in the given place. The duplicate of the resolution ordering the interim measure must be sent to the participants in the proceedings or representatives thereof and those on whom an obligation has been imposed by the interim measure within 3 days following resolution declaration or, if not declared, within 3 days following the issue thereof. Participants other than the plaintiff will be delivered the resolution duplicate and the interim measure proposal.[73]

---

69 Code of Civil Procedure Section 75b.

70 Project Chocen.TV https://www.facebook.com/ChocenTV (29.09.2015).

71 Přenos z kamery u nádraží? Podle správců železnice bezpečnostní hrozba, idnes.cz, 08.07.2015, http://ekonomika.idnes.cz/szdc-zakazala-provoz-webove-kamery-u-nadrazi-v-chocni-pd6-/eko-doprava.aspx?c=A150707_164759_eko-doprava_suj (29.09.2015).

72 Code of Civil Procedure Section 76.

73 Code of Civil Procedure Section 76c.

The resolution ordering the interim measure will be **enforceable by the declaring thereof**. If not declared, it is enforceable as soon as it has been issued or as it has been delivered to the one on whom an obligation is imposed thereby.[74]

The interim measure will **expire if the plaintiff has failed to file** a proposal for proceedings initiation in the statutory period or in the period set out by the court, the proposal in the given matter has not been granted, the proposal in the given matter has been granted and fifteen days following the matter decision enforceability have expired or the specified time for which the interim measures were to last has expired.[75] **The presiding judge abolishes the interim measure** if reasons for which it had been ordered no longer exist. The presiding judge also abolishes the interim measure if the plaintiff has failed to pay the supplement on security within the determined term.

If the ordered interim measure has expired or been abolished for a reason other than because the proposal regarding the given matter has been granted, or because the right of the plaintiff has been satisfied, **the plaintiff is obliged to compensate for damage** and any other loss to anybody to whom the damage or loss has been caused as a result of the interim measure. The plaintiff may not be released from this liability unless the damage or any other loss has also been caused in any other way.[76]

4. General Monitoring of Internet

There is **no Czech legislation on general monitoring of the content of internet**. Nevertheless, if there is a criminal proceeding for a particularly serious criminal offence or any other intentional criminal offence where the prosecution is stipulated in an international treaty, an order for **monitoring of telecommunications may be issued. However, it may be reasonably expected** that it will aid in obtaining all the facts relevant to the criminal proceeding and there is no other way to achieve the purpose, or if it otherwise significantly reduces its achievement.[77] The Police of the Czech Republic performs the monitoring of telecommunications for the needs of all law enforcement authorities.[78] The monitoring of telecommunications traffic between the defence counsel and the accused is inadmissible.[79]

The presiding judge and, in preliminary proceedings upon the petition of the public prosecutor, the judge, is entitled to warrant monitoring. If there is a criminal proceeding for an intentional criminal offence, the prosecution of which is governed by the applicable international treaty, the order for the **monitoring of telecommunications must be issued in writing and must be justified**, including a

---

74 Code of Civil Procedure Section 76d.

75 Code of Civil Procedure Section 77.

76 Code of Civil Procedure Section 77a.

77 Code on Criminal Procedure Section 88.

78 See Pošíková L., Získávání telekomunikačních dat jako nástroj v boji s intenretovou kriminalitou, in Kybernetická kriminalita, Iuridica 4/2012, Acta Universitatis Carolinae, Praha 2013, p.49. See also Profant O., Pirátský zastupitel k hacknutí Hacking teamu: řešení je Otevřená bezpečnost, piratskelisty.cz, 20. 07. 2015, http://www.piratskelisty.cz/clanek-1429-piratsky-zastupitel-k-hacknuti-hacking-teamu-reseni-je-otevrena-bezpecnost (29.09.2015).

79 If the police authority finds during the interception and recording of telecommunications that the accused has communicated with their defence counsel, they are obligated to immediately destroy the records and information learned in this context and they are not allowed to use it in any way. The transcript on the destruction of the record must be filed.

specific reference to the applicable international treaty. This information is considered confidential and is not published.[80]

The order for the monitoring of the telecommunications service must include a determined user address or a user device and the user if their identity is known. At the same time it must include the period during which the monitoring of telecommunications traffic is conducted **cannot be longer than four months**; the justification must include the specific facts that justify the issue of such order as well as its period. **The order for the monitoring of telecommunications** will immediately be forwarded to the police authority. In the preliminary hearing, the judge sends a copy of the order for the monitoring of telecommunications to the public prosecutor without undue delay.

The police authority is obliged to continuously assess whether the reasons which led to an order for the monitoring are still valid. **If the reasons have expired**, they are obligated to immediately terminate the interception and recording of telecommunications even before the end of the permitted period. They will immediately notify the presiding judge in writingand in the preliminary hearing, the public prosecutor and the judge.

Based on the assessment of the current course of the monitoring of telecommunications, the judge of a superior court and, in the preliminary hearing upon the petition of the public prosecutor, deputy county court judge may **extend the duration of the monitoring of telecommunications** traffic even repeatedly, however, always only for a maximum period of four months.

The law enforcement authority[81] may, without the order for the interception and recording of telecommunications, order **the monitoring of telecommunications or conduct it themselves if there is a criminal proceeding** for the criminal offence of human trafficking (Section 168 of the Penal Code), the delegation of custody of a child to someone else (Section 169 of the Penal Code), restriction of personal freedoms (Section 171 of the Penal Code), extortion (Section 175 of the Penal Code), kidnapping of a child and persons suffering from a mental disorder (Section 200 of the Penal Code), violence against a group of people or an individual (Section 352 of the Penal Code), or dangerous threats (Section 353 of the Penal Code), if the user of the intercepted unit agrees to such measure.

If the **record of the telecommunications service is to be used as evidence**, it is necessary to accompany it with a transcript, giving the place, time, manner and contents of the record, as well as the authority, which issued the record. The police authority is obligated to label other records, securely store them to protect them against unauthorised misuse, and indicate the place of storage in the transcript. In any other criminal case the recording may be used as evidence if there is a criminal prosecution even in this matter for a criminal offence, or with the consent of the user by the intercepted station.

If the **monitoring of the telecommunications service did not find any facts relevant to the criminal proceedings**, the police authority, after approval by a court and in preliminary hearings, the public prosecutor must **immediately destroy** all records after three years from the final conclusion of the matter. If the police authority was informed of an extraordinary appeal within the set deadline, they

---

80 See the statement of the Czech police: Policie ČR: Šmírovací software jsme koupili, ale vše je tajné, nic neřekneme (Police of the Czech Republic: we bought monitoring software, everything is confidential and we will say nothing), lupa.cz, 7. 7. 2015, http://www.lupa.cz/clanky/policie-cr-smirovaci-software-jsme-koupili-ale-vse-je-tajne-nic-nerekneme/ (29.09.2015).

81 According to the Czech Act on Criminal Procedure Section 12/1 «Law enforcement authorities are understood to be the court, the public prosecutor and the police authority». "Orgány činnými v trestním řízení se rozumějí soud, státní zástupce a policejní orgán."

destroy the records of the monitoring **after the decision** on the extraordinary appeal or after a final conclusion on the matter. The police authority sends a transcript on the destruction of the record of the monitoring to the public prosecutor, whose decision finally concluded the matter. A transcript is also sent to the presiding judge in the first instance in proceedings before the court, for the record on file.

The public prosecutor by whose decision the case was finally concluded and in proceedings before the court, the presiding judge in the first instance **after the final conclusion of the matter**, informs the person, if known, on the ordered monitoring of telecommunications service. The information includes the designation of the court that issued an order for the monitoring of telecommunications service, the duration of the monitoring and the date of the conclusion. Part of the information includes **the instructions on the right to submit, within six months of receipt of this information**, a petition to **review the legality of the order** for the monitoring of telecommunications service to the Supreme Court. The presiding judge passes the information immediately after the final conclusion of the case to the court in the first instance; the public prosecutor will pass the information immediately after the deadline for the review of their decision to the Attorney General.

The presiding judge or the public prosecutor **does not submit such information in proceedings on particularly serious crimes committed by an organised group**, in proceedings on criminal offences committed for the benefit of an organised criminal group, in proceedings for criminal participation in an organised criminal group, or if the criminal offence involved more people and in relation to at least one of them the criminal proceedings have not yet been finally concluded or if it is against the person to whom the information was submitted, is the subject of criminal proceedings, or if providing such information could defeat the purpose of the criminal proceedings, or if it could lead to **threats to national security, life, health, or the rights and freedoms of individuals**.

If facts relevant to the criminal proceedings need to be established and such data is is **subject to telecommunications service confidentiality** or it is subject to the protection of personal and outsourcing data, then the presiding judge and in the preliminary hearings the judge, orders that the **legal or natural persons who performs the telecommunications activity, notifies them and, in preliminary hearings, notifies either the public prosecutor or the police authority**.[82] The order for finding information on the telecommunications service must be given in writing and must be justified.

An order is not required if the user of the telecommunications equipment whom the data on the performed telecommunications service concerns gives an approval for the provision of the information.

5. Assessment as to the case law of the European Court of Human Rights

In the Czech Republic, **no relevant cases are known** on decision to block, filter or take down content of the internet. In our opinion, the Czech law applicable in general to block, filter and take down content of the internet **meets the requirements of foreseeability, accessibility, and clarity** as developed by the European Court of Human Rights. The law provides for the **necessary safeguards** to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights. Everybody has the right to challenge current practice or the actual application of current legislation of the Czech Republic. According to our information, no such case has yet occurred. We therefore believe that the current legislation is in line with current needs and

[82] Code on Criminal Procedure Section 88a.

does not require any urgent changes.[83] As a Contracting State to the ECHR, general safeguards on freedom of expression apply, including in the field of internet.

With respect to the above, we hold the view that the current Czech legislation in this field is sufficient, **meets the requirements for the protection of human rights**, notably freedom of expression and no further specific legislation is required.

Dr. Josef Skala, PhD.
Researcher at the SICL
01.10.2015

[83] Please compare also “Czech Republic", Country Reports on Human Rights Practices for 2014, Bureau of Democracy, Human Rights and Labor, U.S. Department of State, http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?year=2014&dlid=204278#wrapper (29.09.2015).