MASARYK UNIVERSITY
FACULTY OF LAW

Radim Polčák et al.

INTERCEPTION OF ELECTRONIC COMMUNICATIONS IN THE CZECH REPUBLIC AND SLOVAKIA

ACTA UNIVERSITATIS BRUNENSIS

IURIDICA
Editio Scientia vol. 573

PUBLICATIONS
OF THE MASARYK UNIVERSITY

theoretical series, edition Scientia
File No. 573

INTERCEPTION OF ELECTRONIC COMMUNICATIONS IN THE CZECH REPUBLIC AND SLOVAKIA

This book is based on comparative report that was developed within the research project "INTLI – International Cooperation Lawful Interception" under the direction of the German Centre of Strategy and Research Telecommunication - SFZ TK (Mr. Christian Foerster) in cooperation with Max Planck Institute for Foreign and International Criminal Law (Prof. Dr. Dr. h.c. mult. Ulrich Sieber).

INTERCEPTION OF ELECTRONIC COMMUNICATIONS IN THE CZECH REPUBLIC AND SLOVAKIA

Radim Polčák et al.

Masaryk University
Brno 2016

Vzor citace:
POLČÁK, Radim et al. *Interception of Electronic Communications in the Czech Republic and Slovakia*. 1st edition. Brno : Masaryk University, 2016. 241 p. Publications of the Masaryk University, theoretical series, edition Scientia, File No. 573. ISBN 978-80-210-8423-0.

CIP - Katalogizace v knize

Polčák, Radim
Interception of Electronic Communications in the Czech Republic and Slovakia / Radim Polčák et al. -- 1st edition. -- Brno: Masaryk University, 2016. 241 p. -- Publications of the Masaryk University, theoretical series, edition Scientia ; File. No. 573. ISBN 978-80-210-8423-0 (brož.)

347.77/.78:004* 351.817* 004.6.056.5* 342.721* (437.3)* (437.6)* (048.8:082)*
- právo informačních technologií
- elektronická komunikace
- ochrana dat
- ochrana osobních údajů
- Česko
- Slovensko
- kolektivní monografie

347.7 – Obchodní právo. Finanční právo. Právo průmyslového vlastnictví. Patentové právo. Autorské právo [16]

This publication was created at the Masaryk University in the course of Specific Research Project "Interception of Electronic Communication in the Czech Republic and Slovakia" No. MUNI/A/1153/2015 thanks to the subvention provided by the Ministry of Education, Youth and Sports of the Czech Republic in the year 2016. We would like to express our gratitude.

Text of this work was also published as a chapter in the publication Sieber, U., von zur Mühlen, N. (eds.) *Access to Telecommunication Data in Criminal Justice*. Berlin: Duncker & Humblot, 2016, pp. 247-435. Strafrechtliche Forschungsberichte. ISBN 978-3-428-15143-1.

Validity of the legal text was confirmed on 31 December 2016.

Accessibility of electronic sources was verified on 31 December 2016.

Reviewer: Dr. Tatiana Tropina

Authors: Mgr. MgA. Jakub Míšek, Chapter 1
Assoc. Prof. JUDr. Radim Polčák, Ph.D., Chapter 2
Mgr. Václav Stupka, Chapter 3–6
Mgr. Pavel Loutocký, BA (Hons), Chapter 7
Mgr. Tomáš Abelovský, Chapter 8

ISBN 978-80-210-8423-0

TABLE OF CONTENTS

1 SECURITY ARCHITECTURE AND THE INTERCEPTION OF TELECOMMUNICATION

1.1 National Security Architecture – Two Frameworks of Interception

One of the most important forming factors of the distribution of public powers in the Czech Republic is its totalitarian history. There is a strong sense of distrust towards official institutions in the general public.[1] It is probably due to this fact, that the procedures and powers of public bodies and agencies are set very rigidly. The principle of legality is set in Art. 2 para. 3 of the Czech Constitution (Act No. 1/1993 Sb. Constitution of the Czech Republic), which states that "*State authority is to serve all citizens and may be asserted only in cases, within the bounds, and in the manner provided for by law*"[2] and in Art. 2 para. 2 of the Charter of Fundamental Rights and Freedoms (the Resolution of the Presidium of the Czech National Council of 16 December 1992 on the declaration of the Charter of Fundamental Rights and Freedoms as a part of the constitutional order of the Czech Republic No. 2/1993 Sb.), which states that "*State authority may be asserted only in cases and within the bounds provided for by law and only in the manner prescribed by law*".[3] Since all the public authorities authorized to intercept telecommunication fall within the scope of these articles, they are permitted to act only within the framework of what is expressly allowed for them by law.

In the Czech Republic, there are two frameworks under which electronic communications can be intercepted. The first is the framework of criminal

1 See for example Bobek, M., Molek, P., Šimíček, V. *Komunistické právo v Československu*, Brno: Masarykova univerzita, 2009, 1005 p.

2 English translation taken from the webpage of the Czech Constitutional Court. Online: http://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/Ustava_EN_ve_zneni_zak_c._98-2013.pdf.

3 English translation taken from the webpage of the Czech Constitutional Court. Online: http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Pravni_uprava/AJ/Listina_English_version.pdf.

procedure conducted by the police force, including a special regime of customs service, and the second is a framework of civil and military intelligence services.

The Police of the Czech Republic was established by Act No. 273/2008 Sb. on the Police of the Czech Republic. Among its other duties, it is the main public authority for criminal investigation. It is organized on a geographical basis, as it is organized into divisions according to the administrative regions. There are also several divisions with a countrywide authority.[4] Of those, the most relevant Czech Police divisions for this report are the National Antidrug Central,[5] the Division for Uncovering of Corruption and Financial Criminality,[6] the Division for Uncovering of Organised Crime,[7] and the Unit for Special Activities of Criminal Police and Investigation.[8]

The Czech Police cannot use electronic communication interception as a preventive measure, since the law does not expressly allow it. This is due to the fact that Czech constitutional law strongly protects the privacy of an individual, and interception of communication is seen as a serious breach of such protection.[9] The law therefore provides quite a rigid formulation of exceptions from this protection. Czech criminal procedure is governed by Act No. 141/1961 Sb. Code of Criminal Procedure. According to the Code of Criminal Procedure communication may be intercepted only after the criminal proceedings have started. In the Czech Republic the initial part of criminal proceedings is the preliminary hearing and, as is stated in Section 158 of the Code of Criminal Procedure, it is commenced either

4 In Czech: http://www.policie.cz/clanek/utvary-s-pusobnosti-na-celem-uzemi-cr-312510.aspx.

5 In Czech: www.policie.cz/narodni-protidrogova-centrala-skpv.aspx.

6 In Czech: http://www.policie.cz/clanek/uokfk-skpv-utvar-odhalovani-korupce-a-financni-kriminality-skpv.aspx.

7 In Czech: http://www.policie.cz/clanek/vitam-vas-na-strankach-utvaru-pro-odhalovani-organizovaneho-zlocinu-570688.aspx.

8 In Czech: http://www.policie.cz/clanek/utvar-zvlastnich-cinnosti-sluzby-kriminalni-policie-a-vysetrovani-716842.aspx.

9 For example, the Czech Constitutional Court formulates the importance of this protection in Decision of the Constitutional Court file number II. ÚS 502/2000, N 11/21 SbNU 83, followed by Decision of the Constitutional Court file number II. ÚS 615/06-1, N 88/45 SbNU 291, in which necessary conditions for allowing the interception of communication were interpreted.

when a criminal report is submitted by a citizen, or by the police authority itself as an *ex officio* act. Once the criminal proceedings have started and the legal prerequisites are met, the Police can commence with the interception.

A specific example of interception in accordance with the Code of Criminal Procedure is a communication interception, which is grounded in Act No. 17/2012 Sb. on the customs service of the Czech Republic. The customs service can, in certain cases, be considered a police force and can act in accordance with the rules of criminal proceedings for obtaining authorisation to conduct interception. Section 63 of Act No. 17/2012 Sb. specifies the cases over which the customs service has jurisdiction. It is interesting to point out that this can be understood as a preventive measure. The use of this provision is, however, strictly limited by the purpose of the interception, which is set out in paragraph 1 of Section 64 that reads as follows:[10]

> *"Section 64*
>
> *(1) Usage of operative search means must not follow any other purpose than the one, which is specified in the concerned international treaty. Rights and freedoms of intercepted persons can be restrained on in the necessary manner."*

The Czech Republic has three intelligence services: The Office for Foreign Relations and Information (foreign intelligence service), the Security Information Service (interior counter-intelligence service) and the Military Intelligence. They are strictly separated from one another. This separation can again be interpreted as a result of the Czech totalitarian history and the general distrust towards public institutions, especially those with executive power of this kind. *Lex generalis* covering these services is Act No. 153/1994 Sb. on intelligence services of the Czech Republic; the special acts are Act No. 154/1994 Sb. on the Security Information Service and Act No. 289/2005 Sb. on Military Intelligence. The rules for communication interception conducted by intelligence services are included in these acts.

A specific case connected with the intelligence services is the National Security Authority,[11] an institution responsible for personnel and facility security clearance procedures. It has overall competences in the area of protection of classified information and, among other things, it issues personnel security

10 Section 64 of Act No. 17/2012 Sb. on the Customs service of the Czech Republic.
11 Http://www.nbu.cz/en/.

clearance certificates. It is governed by Act No. 412/2005 Sb. on protection of secret information and security. Section 107 para. 3 of this act, which covers personal security clearance procedures, empowers the National Security Authority to ask an intelligence service to carry out an examination of possible security risks in the candidate's surroundings for clearance purposes: [12]

> *"Section 107*
>
> *Acts in the proceeding on issuance of personnel security clearance certificates*
>
> *(3) In the proceedings on issuance of personnel security clearance certificates for the Top Secret degree the Office*[13] *shall conduct all the acts according to the paragraph 2 and furthermore it requests competent intelligence service to conduct an examination of possible security risks in the environment, in which the subject operates."*

This issue can be summed up as follows: There are two different and separate frameworks of communication interception in the Czech Republic. Each of them has a different purpose and a different approval procedure and thus, generally speaking, information gained within one framework cannot be easily used in another.

1.2 Powers for interception of telecommunication – Legislative grounds

1.2.1 The law of criminal procedure

The interception of communication can be used for the sake of criminal proceedings only when the criminal proceedings are conducted for crimes that are specifically listed by the law. The general rule is that the interception must be initially authorized by a judge but, in certain cases, which are laid down in Section 88 Para. 5 of the Code of Criminal Procedure, prior consent of the person using the intercepted unit is sufficient.

The strict nature of this authorisation process was confirmed by the Czech Constitutional Court in Decision file number II. ÚS 615/06-1 of 23 May 2007. The court wrote the following in its decision:

12 Section 107 paragraph 3 of the Act No. 412/2005 Sb. on protection of secret information and security. Informal translation by the author of this chapter.

13 That is The National Security Authority.

"The right to protection of the secrecy of messages arising from Art. 13 of the Charter of Fundamental Rights and Freedoms, together with personal freedom and other constitutionally guaranteed fundamental rights, comprises the personal sphere of an individual, whose individual integrity, as an essential condition for a dignified existence and the development of human life generally, must be respected and thoroughly protected as a token of respect for the rights and freedoms of people and citizens.[14]

If the constitutional order permits a breach of this protection, it does so solely and exclusively in the interests of a democratic society, or in the interest of the constitutionally guaranteed fundamental rights and freedoms of others… Therefore, there may be only such infringement of the fundamental rights and freedoms by the state power, which is necessary in this sense.[15]

It should be emphasized that an effective judicial review of the use of any operative means, with an overlap into the area of fundamental rights and freedoms, is absolutely crucial to a fair trial in criminal proceedings.[16]

In terms of the constitutional order, a violation of the secrecy of messages is possible only in cases and manner prescribed by law. Statutory regulation interfering with this right must be formulated so that it does not deny this fundamental human right and it must also be interpreted this way… A court order for interception and recording of telecommunication operations must be written and reasoned. It must therefore be issued in respect to a person against whom criminal proceeding is conducted. If the proceedings are conducted on the basis of reasonable suspicion, it must be explained in a recital what evidence supports such conclusion. The mere criminal complaint itself, if it does not include explanation, is not sufficient for court order… The order may therefore be issued only in duly commenced criminal proceedings for a legally qualified crime, and must be supported by relevant clues from which we can derive a reasonable suspicion of committing such a crime. The order must be individualized in a relation to the specific person who is the user of intercepted telephone device… Finally, the order must provide at least a minimal indication of what facts relevant for the proceeding are to be thus identified, and what is inferred from that.[17]*"*

This strict approach was also acknowledged in Art. 67 of Internal Order of the Police President No. 30/2009 of 21 April 2009 on the fulfilment

14 Decision of the Constitutional Court file number II. ÚS 615/06-1, N 88/45 SbNU 291.
15 Ibid, paragraph 14.
16 Ibid, paragraph 15.
17 Ibid, paragraph 16.

of operations in criminal proceedings,[18] which was repealed by the Order of the Police President No. 103/2013 on the fulfilment of certain operations of the bodies of Police of the Czech Republic in criminal proceedings.[19]

Outside the regime of criminal procedure, the Police can conduct communication interception when supervising a person protected in the special framework of witness protection. This is done in accordance with Section 10a of Act No. 137/2001 Sb. on special protection of a witness and other persons in connection with criminal proceedings. This interception can be commenced only after prior judicial authorisation.

The collection of traffic and location data by providers of electronic communications (data retention) and the option for the Police to access such data during criminal proceedings is laid down in Section 88a of Act No. 141/1961 Sb. Code of Criminal Procedure. In the cases enumerated in the paragraph 1 of the section police can gain access to traffic and location data after a preliminary judicial authorisation.

A general authorisation for the Czech Police to access location and traffic data is laid down in Section 66 para. 3 of Act No. 273/2008 on the Police of the Czech Republic: [20]

> *"Section 66*
>
> *Obtaining information from records and databases*
>
> *(1) Police may, in cases prescribed by law and to the extent necessary to fulfil a specific task, request a legal or natural person providing a public communications network or publicly available electronic communications with the traffic and location data in a manner, which enables remote and continuous access, unless another law provides otherwise. These persons are obliged to grant the request without undue delay, as and to the extent determined by other legislation."*

However, there are three situations in which the Czech Police can access location and traffic data even outside the framework of criminal procedure.

18 Available in Czech online: http://www.pecina.cz/files/pokyn2.pdf.

19 Even though the order No. 103/2013 is not publicly available, it is assumed that discussed issue is regulated in the same way, as it was in the order No. 30/2009.

20 Act No. 273/2008 on the Police of the Czech Republic.

The first situation concerns the search for persons and things. This authorisation to access traffic and location data is established in the second paragraph of Section 68 of the Police Act.[21]

> *"Section 68*
>
> *Search for persons and things*
>
> *(2) Police can request legal or natural person providing a public communications network or publicly available electronic communications service traffic and location data in a manner enabling remote and continuous access, for a purpose of ongoing search for wanted or missing persons and for the purpose of identifying a person of unknown identity or the identity of the found corpse, unless another law provides otherwise. The information is provided in the form and to the extent determined by other legislation."*

An interesting fact is that location and traffic data can be accessed without prior judicial authorisation within this framework.[22] This statement is also true for the second situation, which is access to location and traffic data for the purpose of fighting against terrorism and preventing specific terrorist threats as laid down in Section 71 of the Police Act.

The fact that location and traffic data can be accessed without prior judicial authorisation and the lack of other checks and balances[23] gives the Police a powerful instrument, which could be easily abused by collecting a disproportionate amount of data. This could lead to a serious threat to personal data and privacy.[24]

---

21 Act No. 273/2008 on the Police of the Czech Republic.

22 For more detail, see Myška, M. *Právní aspekty uchovávání provozních a lokalizačních údajů*, Brno: Masarykova univerzita, 2013, 133 s.

23 Section 11 of the Police Act sets a general principle of proportionality; however, it is our opinion that this general provision is not a sufficient insurance that the legal authorisation to collect such data will not be abused. See more e.g. Vangeli, B. Zákon o Policii České republiky, Praha: C. H. Beck, 2014, p. 64.
"Section 11 Adequacy of the procedure
A policeman and police employee are required to ensure that no person suffered unwarranted injury due to their actions,
ensure that their decision not to act did not resulted in unsubstantiated harm to persons whose security is endangered,
proceed in a way that any possible interference with the rights and freedoms of persons to whom the act is directed, or any others, did not exceed what is necessary to achieve the objective pursued by the act."
Act No. 273/2008 on the Police of the Czech Republic.

24 See more e.g. Myška, M. *Právní aspekty uchovávání provozních a lokalizačních údajů*, Brno: Masarykova univerzita, 2013, 133 s.; Harašta, J., Myška M., Budoucnost data retention, *Trestněprávní revue*, 2015, Vol. 14, No. 10, pp. 238-241.

The last situation, in which the Police can access traffic and location data outside the criminal proceedings involves supervision over a person protected by the special programme of witness protection. Similar to communication interception, this permission is regulated by Section 10a of Act No. 137/2001 Sb. on special protection of a witness and other persons in connection with criminal proceedings. In this case, prior judicial authorisation is necessary to access traffic and location data.

1.2.2 Law of intelligence agencies

Generally speaking, the conditions, which need to be met in order to legally carry out communication interception within the framework of intelligence agencies, are less strict than those for interception in criminal proceedings.

The wording of statutory authorisation to conduct communication interception in Acts No. 154/1994 Sb. on the Security Information Service and No. 289/2005 Sb. on Military Intelligence is practically identical. In both acts, the interception is grounded in Sections 8 and 9.[25]

The Office for Foreign Relations and Information is not expressly authorized by law to conduct communication interception. It is out of the scope of its competence, since the information collected by means of interception would be from within the borders of the Czech Republic. However, should the Office need to conduct such an interception, it can request it to be carried out by other intelligence services, most likely the Security Intelligence Service. This can be done on the basis of Section 9 of Act No. 153/1994 Sb. on intelligence services of the Czech Republic, which allows cooperation between services based on an agreement between them: [26]

> *"Section 9*
>
> *Intelligence services cooperate with each other on the basis of agreements, which are concluded with the consent of the Government."*

Such interception would be completely within the legal framework of Act No. 154/1994 Sb. on the Security Information Service.

---

25 The provision, which is marked as the paragraph 5 of section 9 of the Act No. 154/1994 Sb. on Security Information Service, is equivalent to Section 8a of the Act 154/1994 Sb. on Security Information Service.

26 Act No. 153/1994 Sb. on intelligence services of the Czech Republic

Even though the intelligence service needs a judicial approval for conducting communication interception, just as it is needed in criminal proceedings, it is not limited to specific situations like the investigation of a crime enumerated in the statue. It is therefore legally easier to obtain such approval. This difference was elaborated by the Czech Constitutional Court in Decision file number I. ÚS 3038/07, N 46/48 SbNU 549, from 29 February 2008 in which the Court stated that information obtained from communication interception by an intelligence service cannot be freely used in criminal proceedings.[27] According to the Constitutional Court in this case, there is a difference in the purposes of the two frameworks for communication interception. In the case of the criminal proceedings framework, the entire process is contained within the judiciary branch of the state power, its purpose being solely the solving of a crime; the evidence is obtained by the Police based on the rules laid down in the Code of Criminal Procedure and subject to a closer judicial review. On the other hand, the intelligence framework is rooted in the executive branch of state power, its purpose being national security; the judicial review is much less extensive than in the case of criminal proceedings. In paragraph 29, the Court states: "*Intelligence service interceptions do not reach the guaranteed quality, which is required by the Code of Criminal Procedure, and therefore they cannot be used in the criminal proceedings, because they were not obtained in a legal manner.*"[28]

1.2.3 Financial and Customs Investigation Service

As discussed above, in the first subsection of this chapter, the legal framework for communication interception for the customs investigation service specifically is stipulated in Section 63 of Act No. 17/2012 Sb. on customs service of the Czech Republic. This section, however, does not establish a new unique framework for message interception. It is only a specification of the criminal

27 In this case, the criminal proceedings against the defendant were commenced after the police obtained a military intelligence recording obtained by intercepting communication to which the defendant was party. She was, however, not a legitimate subject of the interception. She issued a complaint against the commencement of the criminal proceedings, which was denied by the public prosecutor. After a series of appeals, the Constitutional Court ruled in her favour.

28 Paragraph 29 of the decision of the Czech Constitutional Court file number I. ÚS 3038/07, N 46/48 SbNU 549.

procedure framework, since the customs service may serve as a police force in the first phase of the criminal proceedings, the preliminary hearing. That is, however, only in the situation described in the above-mentioned Section 63.

Aside from the Police and the intelligence services, another institution that can request access to traffic and location data is the Czech National Bank. This can be done as part of its responsibility for supervising the capital market, and prior judicial authorisation is required. The Czech National Bank is entitled to request the data directly from providers of electronic communications services, without the use of police services.

1.3 Responsibility for the technical performance of interception measures – a general overview

In the Czech Republic, the technical implementation of communication interception is carried out by state agencies, with the cooperation of legally bound subjects, in accordance with Act No. 127/2005 Sb. on electronic communication. Section 97 para. 1 of the Electronic Communications Act establishes a duty for any legal or natural person providing a public communications network[29] or a publicly available electronic communications service[30] to provide and secure interfaces at specific points of the network for connection of terminal equipment for message tapping and recording. This is done at the requesting party's expense. This section authorizes the Police of the Czech Republic, the Security Information Service, and the Military Intelligence to do so.

The access to traffic and location data is laid down in Section 97 para. 3 in a similar fashion. This provision authorises public authorities involved in the criminal proceedings, the Police (for conducting a search for missing persons and things and the prevention of terrorist activities), the intelligence

29 Section 2 letter j) defines the public communication network as "an electronic communications network which is used wholly or mainly for the provision of publicly available electronic communications services and which supports transmission of information between end nodes of the network or an electronic communications network via which is provided service of television or radio broadcasting."

30 Section 2 letter o) defines the publicly available electronic communications service as "electronic communications service from the use of which no person is excluded beforehand."

services, and the Czech National Bank to request the legal or natural person providing a public communications network or a publicly available electronic communications service to provide traffic and location data.

When it comes to the criminal procedure framework of communication interception, the Unit for Special Activities[31] (a division with countrywide authority) is the only division of the Czech Police authorized to conduct interception operations. A detailed procedure for this process is set out by the Order of the Police President No. 186/2011 upon request for tapping and recording of telecommunication traffic and upon request for traffic and location data, which was amended by the Order of the Police President No. 139/2012. This order is unfortunately not publicly accessible. However, the technical and request process is quite well described in the document "Analysis of tapping and recording of telecommunication traffic," which was published by the Police Presidium of the Czech Republic on 6 June 2014.[32]

When the conditions of Section 88 para. 1 are met, the authorized person, i.e. the policeman working the criminal case, can request the interception. This request must contain a brief summary of the factual situation of the case and a justification for the request. Most importantly, it must contain the facts that are expected to be uncovered through the interception, which must be important for the case. Furthermore, the request must include an identification of the user unit that is to be intercepted (number, address, and name of its user, if known) and the period of time for which the interception should be conducted. This period may be no longer than four months. Before approval of the request, a designated officer of the Unit for Special Activities must be consulted; he or she will then evaluate the request from a technical and operative point of view and decide whether the interception is possible and doable.[33]

If the criminal proceedings are in the preliminary hearing phase, the request is send to the Public Prosecutor, who then requests the interception from

31 The webpage of the division in Czech: http://www.policie.cz/clanek/utvar-zvlastnich-cinnosti-sluzby-kriminalni-policie-a-vysetrovani-716842.aspx.

32 In Czech online: www.mvcr.cz/soubor/ppr-102-31-cj-2014-990390-analyza-odposlechu-a-sledovani-za-rok-2013-pdf.aspx.

33 *An analysis of the tapping and recording of telecommunication traffic*, p. 16.

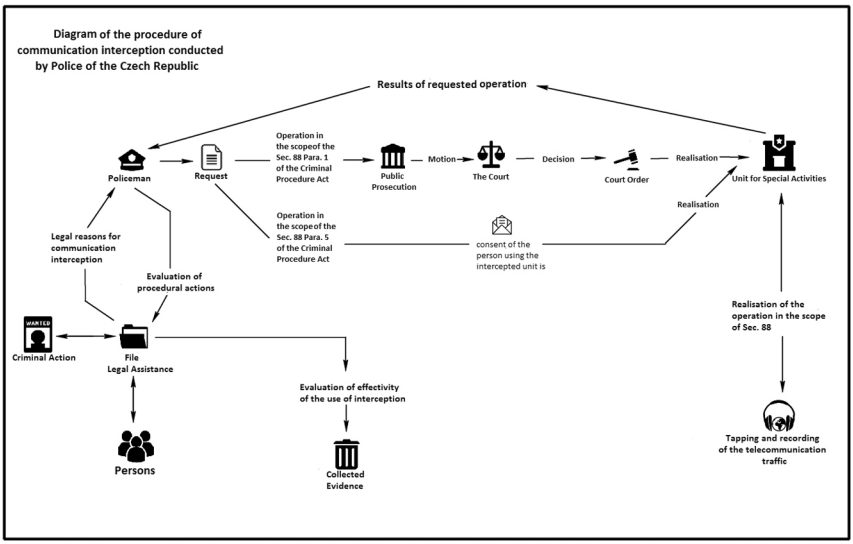
the court. In the later phases of the proceedings, the court can be contacted directly. The court then issues a decision, namely a court order, which is delivered back to the Public Prosecutor (preliminary hearing) or directly back to the authorized person, who then delivers it to the Unit for Special Activities. When the conditions of Section 88 para. 1 are met, the authorized officer must obtain consent from the person using the intercepted unit. Once again, a properly filled out request is delivered to the Unit for Special Activities. In both situations, the Unit conducts the requested communication interception and the result of it, which is a sound recording recorded on a non-rewritable medium, is delivered back to the authorized person, who issued the request in the first place.

The court order must be specific and justified, including for example a reference to a specific international treaty, should the interception be conducted in the context of an intentional criminal offense, for which the prosecution is stipulated in a declared international treaty. The order must contain specific identification of the intercepted unit (the address and identity of its user, if known) and the time period for which the interception is authorized.

After the end of the interception, the police institution has a short time to evaluate the recordings and insert statistical data into a specialized system, MU II. If the recordings are not going to be used in the criminal proceedings, they must be destroyed three years after the proceeding has legally ended.

If the recording of the telecommunication service is to be used as evidence, it is necessary to provide a transcript for it, stating the place, time, manner, and contents of the record, as well as the authority that issued the record. The police authority is obliged to label other records, securely store them to protect them against unauthorized use, and indicate the place of storage in the transcript. In a criminal case other than that for which the interception and recording of the telecommunication service was performed, the recording may be used as evidence if there is a criminal prosecution in this matter for a criminal offense referred to in Para. 1 of Section 88 or with the consent of the user of the intercepted station or device.

The following diagram shows the request procedure for the authorisation of communication interception.[34]



Section 19 of Act No. 273/2008 on the Police of the Czech Republic authorizes the police forces to provide technical support and conduct communication interception for another public authority upon request and only when that body is authorized to perform such action. The other public authority must declare this fact in its request.

This is the case for the customs service, since, even though it is authorized by Section 63 of the Act on Customs Service of the Czech Republic to use communication interception, Act No. 127/2005 on electronic communications does not set a duty for electronic communications providers to allow the customs service access to their networks. Customs therefore use the services of the Police (and therefore the Unit for Special Activities). However, the general directorate of customs is authorized to secure the application of intelligence techniques, including communication interception (Section 4 para. 5 letter c) of the Customs Service Act), for other public authorities.

34 *Analysis of tapping and recording of telecommunication traffic*, p. 15, edited and translated by the author of the chapter.

Like in the above-mentioned Section 19 of Act No. 273/2005, this can be done upon a request when the other public authority is authorized to perform such action.

Interception of communication can be conducted by intelligence services within their specific legal framework. The rules for communication interception carried out by the Security Information Service and the Military Intelligence are, as could be seen above, almost identical. Both services can request interception from a provider of public electronic communications and both can serve as technical support for other public bodies with authorization to conduct communication interception (Section 9 paras. 4 and 5 of Act No. 289/2005 Sb. on Military Intelligence and Section 8a and Section 9 para. 4 of Act No. 154/1994 Sb. on the Security Information Service).

The judicial authorization procedure is the same for both intelligence agencies and it is laid down in Section 10 of their respective acts (Act No. 289/2005 Sb. on Military Intelligence and Act No. 154/1994 Sb. on the Security Information Service).

An example of a public authority that can request the use of communication interception from the police and intelligence services is the General Inspection of Security Forces. According to Section 9 para. 2 a) of Act No. 341/2011 Sb. on the General Inspection of Security Forces, this authority can request communication interception of Security Forces and other public bodies to be conducted for the purpose of fulfilling its inspection duties. This interception is carried out within the legal framework of criminal procedure, since the request must include authorization issued in a process governed by the Code of Criminal Procedure: [35]

> *"Section 9*
>
> *(3) General Inspection may require from Security Forces and other public authorities, if it is necessary for the performance of a specific task of the Inspection*
>
> *a) technical and personal resources for interception and recording of telecommunication operations or for operative intelligence means. In the request the Inspection demonstrates that the use of interception and recording of telecommunication operations or monitoring people and things have been permitted under the Criminal Procedure Code."*

35 Section 9 of the Act No. 341/2011 Sb. on General Inspection of Security Force.

The Chamber of Deputies of the Czech Parliament is the control body for communication interception for the Police of the Czech Republic (Section 98 of Act No. 273/2008 Sb. on the Police of the Czech Republic) and the customs service (Section 65 of Act No. 17/2012 Sb. on the customs service of the Czech Republic). The Chamber of Deputies is also a control body for intelligence services in general (Section 21 of the Military Intelligence Act and Section 18 of the Security Information Service Act); however, supervision of specific communication interceptions is done by the courts (Section 11 of the Military Intelligence Act as well as of the Security Information Service Act).

As was mentioned in the second part of this chapter, the general authorization for the Police of the Czech Republic to request access to traffic and location data from electronic communications providers is found in Section 66 para. 3 of Act No. 273/2008 Sb. on the Police of the Czech Republic. The general authorization for the intelligence services to access such data is found in Section 8a of Act No. 154/1994 Sb. on the Security Information Service and in Section 8 para. 5 of Act No. 289/2005 Sb. on Military Intelligence. The authorization for the Czech National Bank to access such data is found in Section 8 of Act No. 15/1998 Sb. on supervision in the area of capital market and change and supplementation of some acts.

1.4 Legitimacy of data transfers between different security services

Generally speaking, the situation in the Czech Republic is similar to the situation in Germany because the frameworks and functions are separate from one another. There are several reasons for this. The first one is the abovementioned strong principle of legality. If the possibility of data transfer and sharing of information is not expressly written in the law, the agency cannot use information collected by another agency. If the possibility of information transfer is written in the law, it can be done only within the scope of the legal permission. The second reason for the separation is that different agencies intercept communication for different purposes and thus the process of obtaining permission for such interception also differs. Should the information be used in another framework than that for which they were

collected, especially when the interception conducted by the intelligence service is to be used in criminal proceedings, it would be considered unlawful evidence and as such it would not be admissible by the court. In paragraph 25 of the above-mentioned Decision file number I. ÚS 3038/07 from 29 February 2008,[36] the Czech Constitutional Court states that of the fact that the Code of Criminal Procedure is silent in the matter of the option of using a communication interception obtained by a body other than the Police, or not obtained in compliance with the Code of Criminal Procedure, as evidence in criminal proceedings needs to be interpreted in the light of the principle of legality, meaning that such interception cannot be used as evidence.

For example, intelligence services have a general authorisation to pass on data in the section 8 paragraph 3 of the Act No. 153/1994 Sb. on intelligence services of the Czech Republic. The intelligence service must provide information to other public bodies and police forces – specifically the findings that fall within their jurisdiction. It is not, however, permitted to pass on too much of specific information, since that would be a violation of the principle of legality, as stated by the Czech Constitutional Court in paragraph 28 of the above-mentioned Decision file number I. ÚS 3038/07.[37]

Passing on information within different intelligence services is not expressly covered by the law; therefore, it can only be carried out within the scope of the general provision.

Furthermore, there are no specific provisions that expressly allow data to be passed from communication interception to intelligence services. However, there are authorisations for passing on information in general. This authorisation is not so specific and strong, so the principle of legality could be breached should it be used disproportionally.

For the Police, the authorisation is laid down in Section 78 of Act No. 273/2008 Sb. on the Police of the Czech Republic. This section allows the Police to hand over information, which was acquired during the fulfilling of their duties, to the national member of the Eurojust, the National Security Office, the intelligence services of the Czech Republic, the Military

36 Paragraph 25 of the decision of the Czech Constitutional Court file number I. ÚS 3038/07, N 46/48 SbNU 549, online: http://nalus.usoud.cz.

37 Ibid, paragraph 28.

Police, the Ministry of the Interior and other public bodies, should it be necessary for services in their jurisdiction.

A very similar authorisation as this one can be found in the section 57 of the Act on Customs service of the Czech Republic (Act No. 17/2012 Sb.). This section authorizes customs services to pass on information to the same degree as the above-mentioned Section 78 for the Police.

The same scope also covers Section 37 of the Act on the General Inspection of Security Forces (Act No. 341/2011 Sb.), which authorizes the General Inspection to pass on information to other public bodies.

1.5 Statistics on Telecommunication Interception

In Czech law is not present an obligation to collect and create statistics on telecommunication interception. However, the Police compile statistics based on the order of the Police President No. 31/2012 on the analytical and statistical information system MU II. This order is, unfortunately, not publicly available.

The Czech Police publish statistical reports on the use of electronic interceptions and the interception of people and things. The most recent one is a report from 2013, which was published on 6 June 2014.[38] These statistics include only the communication interception conducted within the framework of criminal proceedings under the provision of Section 88 of Act No. 141/1961 Sb. Code of Criminal Procedure. Communication interception by intelligence services and customs in accordance with their special legal regulation is therefore not included in these statistics. No statistics on these kinds of communication interceptions are publicly accessible.

The following information has been taken from the police statistics, which present for example the absolute number of interceptions, the number of intercepted stations and people, and the differentiation of interceptions according to the type of crime, as well as the overall effectivity of interceptions. The statistics do not, however, distinguish interceptions based on their nature, namely whether they are electronic, meaning for example detection of keystrokes, data tracking, etc. or whether they are telephonic interceptions.

38 In Czech online: www.mvcr.cz/soubor/ppr-102-31-cj-2014-990390-analyza-odposlechu-a-sledovani-za-rok-2013-pdf.aspx.

The following table is a summary of the data taken from the above-mentioned analysis.

	Total	Regional Police Directorates	Office of Criminal Service and Investigation	Division for the Uncovering of Organised Crime	National Antidrug Center	Division for the Uncovering of Corruption and Financial Crime
Processed Criminal Files	135 731	134 923	N/A	184	147	477
No. of criminal files where communication interception could have been used	47 944	47 513	N/A	93	91	247
No. of criminal files where communication interception was used	1175	949	21	93	47	65
Percentage of criminal files where interception was realized to criminal files where it was legally possible to conduct it	2,5 %	2,0 %	N/A	100 %	51,6 %	26,3 %
No. of intercepted telecommunication units	6 689	4 095	51	990	964	589
No. of intercepted persons	4 258	2 581	36	518	628	495
Average no. of units per Person	1,6	1,6	1,4	1,9	1,5	1,2
Average no. of units per Criminal file	5,7	4,3	2,4	10,6	20,5	9,1
No. of units intercepted after authorisation by a judge (section 88, para. 1 of the Code of Criminal Procedure)	6540	3947	51	989	964	589
No. of units intercepted after consent of the intercepted person (section 88, para. 5 of the Code of Criminal Procedure)	149	148	0	1	0	0

The analysis also offers a chart with the data concerning the effectivity of the performed interceptions. There are several categories that are used for this evaluation.

1. Active / Inactive interception
   "Active" refers to interception that was commenced by the Unit for Special Activities of the Criminal Police and Investigation and the information collected. The following categories (Nos. 2, 3, and 4) are subdivisions of this category.
   There are two kinds of "inactive" interception.

a) The Unit for Special Activities of the Criminal Police obtained an authorized request for the interception, the interception was commenced and realized, but no recordings for the criminal procedure were obtained. An example of this situation is that the mobile phone was inactive or the person of interest was not present in the Czech Republic.

b) The Unit for Special Activities of the Criminal Police obtained an authorized request for the interception; however, the interception was not realized. For personal, technical, or other reasons, no actions were taken by the Unit for Special Activities of the Criminal Police for the entire time of the validity of court authorization, and therefore no recordings were collected.

2. Direct influence on the criminal procedure
   The collected information was, or will be, used:

a) As evidence in ongoing criminal proceedings;

b) for tactical reasons and further investigation;

c) to prevent another crime;

d) to capture a criminal offender.

3. Indirect influence on the criminal procedure
   The collected information was, or will be, used for a discovery of:

a) A new criminal activity on the part of the criminal offender who was subject to the interception;

b) a new criminal activity on the part of third persons who were not initially subject to the ongoing interception.

4. Information obtained via the interception was not used.

   This category covers interception that was ineffective, because it did not lead to any information that could be used in the criminal procedure.

	Total	Regional Police Directorates	The Office of Criminal Service and Investigation	Division for the Uncovering of Organised Crime	National Antidrug Center	Division for the Uncovering of Corruption and Financial Crime
No. of intercepted telecommunication units	6689	4095	51	990	964	589
Inactive interception	578	386	0	27	126	39
Direct influence on the criminal procedure only	4123	2176	47	759	736	406
Indirect influence on the criminal procedure only	15	15	0	0	0	0
Combination of direct and indirect influence on the criminal procedure	1081	898	0	110	36	37
Information obtained via the interception not used	891	620	4	94	66	107

In 2013, the average length of interception was 97.26 days.[39]

When compared with previous years, an increasing tendency in the number of communication interceptions can be seen starting in 2009.

	2006	2007	2008	2009	2010	2011	2012	2013
No. of intercepted units	7599	5491	4973	4571	5006	5766	6241	6689

39 Analysis of tapping and recording of telecommunication traffic. Police Presidium of the Czech Republic. 2014, p. 80.

2 CONSTITUTIONAL AND STATUTORY SAFEGUARDS OF TELECOMMUNICATIONS

2.1 Areas of constitutional protection

Apart from the constitution itself, the Czech Republic also has other documents that together form the Czech constitutional black-letter law: these are the constitutional laws and the Charter of Fundamental Rights and Freedoms. Together, these documents form the Czech Consitutional Order *(Ustavni poradek)*. Basic safeguards for the protection of fundamental rights are laid down in the Charter of Fundamental Rights and Freedoms, which lists all of them and provides brief explanations.

The recently applicable Czech constitutional law (valid since 1993) acknowledges privacy as a distinct distributive (individual) right. Apart from being mentioned in Art. 7(1) of the Charter of Fundamental Rights and Freedoms, it is also laid down specifically with regard to personal life in Art. 10(2), with regards to personal data in Art. 10(3), and with respect to communications and records in Art. 13.[40]

> *"Article 7(1): Inviolability of the person and of privacy is guaranteed. It may be limited only in cases specified by law.*
>
> *Article 10(2): Everybody is entitled to protection against unauthorized interference in his or her personal and family life.*
>
> *Article 10(3): Everybody is entitled to protection against unauthorized gathering, publication or other misuse of his or her personal data.*
>
> *Article 13: Nobody may violate secrecy of letters and other papers and records whether privately kept or sent by post or in another manner, except in cases and in a manner specified by law. Similar protection is extended to messages communicated by telephone, telegraph or other such facilities."*

Privacy is laid down in the aforementioned provisions as a right *per se* (it does not form a subsequent right) that can be claimed individually. This means

40 Resolution of the Praesidium of Czech National Council No. 2/1993 Sb., English translation is available at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Pravni_uprava/AJ/Listina_English_version.pdf.

that privacy as a regulatory phenomenon consists of individualized protective rights that are all subject to judicial protection, but also that whenever privacy is at stake, it should always be possible for an individual to seek direct judicial protection or at least a judicial review of administrative decisions or other regulatory actions.[41]

The secrecy of telecommunication is specifically recognized as a fundamental right in Art. 13 of the Charter of Fundamental Rights and Freedoms (see above). Legislation thereof is analogous to the traditional secrecy of letters, whereas any limitation of this protection has to be based on statutory law. This implies that telecommunication secrecy cannot be limited by bylaws or administrative decisions *per se* – any such limitation has to be grounded in the statutory law.

The fact that the secrecy of telecommunication is recognized by the Charter of Fundamental Rights and Freedoms as an individual right implies that any infringement has to be reviewable by an independent judiciary. Together with the fact that telecommunication secrecy is a highly sensitive issue in the Czech Republic,[42] this principle correspondingly led to currently applicable strict statutory safeguards for wiretapping and similar intrusions of information privacy.[43]

There are no specific constitutional provisions regarding the confidentiality and integrity of information systems. Such protection, however, can be derived from more general fundamental rights. In this respect, it is to be noted that there is a reason to distinguish between the confidentiality and integrity of information systems as such and the confidentiality and integrity of data that are stored or communicated therein.

41 That is based on general Kantian centrality of a person and their rights – see for example Kant, I. The Universal Principle of Right: The Laws of Freedom as Moral, Judicial and Ethical, *Illinois Law Review*, 1914-1915, vol. 9, No. 3, p. 574. The Czech Constitutional Court constantly reflects upon that principle – see e.g. case file number IV.ÚS 412/04, N 223/39 SbNU 353.

42 There are multiple reasons for high public sensitivity to privacy infringements, some of which are grounded in the communist period of the modern history of the Czech Republic. See for example Bobek, M., Molek, P., Šimíček, V. *Komunistické právo v Československu*, Brno: Masarykova univerzita, 2009, 1005 p.

43 For a general explanation of protective tendencies with regards to information privacy in Czech criminal law, see Púry, F. Posílení ochrany informací v trestním řízení, *Právní rozhledy*, 2009, Vol. 17, No. 7, p. II.

In the first case, specific protective tools are correspondingly based on the general protection of property laid down in Art. 11(1), whichreads as follows: *"Everybody has the right to own property. The ownership right of all owners has the same statutory content and enjoys the same protection, inheritance is guaranteed."*

The latter case, i.e. the protection of data stored in information systems, is based on fundamental rights protecting specific types of data. Apart from the protection of privacy and personal data, these might include, e.g. the protection of trade secrets, health records, speech, etc.

The issue of confidentiality and the integrity of information systems is also closely linked to the active component of the concept of informational self-determination (see below). Recently the protection of informational self-determination has served as a constitutional basis for the adoption of the Cybersecurity Act,[44] which is primarily aimed at the establishing of security measures for the protection of the confidentiality, security, and availability of critical information infrastructure.[45]

The term 'privacy' is used in the Czech law in two main meanings of the word. One of them serves as general constitutional principle. Another meaning of the term 'privacy' (soukromi) is primarily found in the Civil Code and it establishes civil remedies for cases of infringement.

In the Czech civil law, privacy protection has been systematically included into a more general category of personality protection (apart from privacy, personality protection also includes the protection of dignity, esteem etc.). When used as a regulatory principle (typically in personal data protection law, the law of electronic communications, criminal procedural law etc.), privacy is generally replaced by a more general term "the right to respect for private life."

The German concept of informational self-determination was adopted into Czech law through decisions of the Czech Constitutional Court.[46] It has

44 Act No. 181/2014 Sb., English translation available at https://www.govcert.cz/download/nodeid-1143/.

45 For a more specific analysis of the Czech cybersecurity legal regulatory framework, see Polčák, R. Kybernetická bezpečnost jako fenomén českého práva, *Revue pro právo a technologie*, 2015, Vol. 11, No. 11, pp. 95-149.

46 For a detailed explanation of the concept, see Schwartz, P. The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 1989, *American Journal of Comparative Law*, Vol. 37, No. 4, pp. 675-701.

recently been used in Czech constitutional practice as a common denominator for various individual information rights.

The Czech Constitutional Court distinguishes between the active and passive component of informational self-determination. The passive component is represented by various individual information rights, which consist of protecting data related to an individual from unlawful interference. The active component of information self-determination is based on the assumption that one cannot live a regular personal life without the ability to actively communicate (i.e. without the possibility to have access to the means of communication established as standard in regular interpersonal exchange of information).

The Constitutional Court used the active component of information self-determination in a case where a woman was sentenced for an economic crime incl. subsequent damages.[47] In the trial, her petition for pro bono legal representation was refused based on the fact that she regularly paid a relatively high fee for her cable TV and Internet connection at home (which was interpreted as a demonstration of the fact that she had sufficient funds to pay for her legal representation). The Constitutional Court held that requiring her to give up her Internet connection would mean disproportionate limitation of her right for information self-determination, since one of its components is also the right to communicate actively. This decision of the Constitutional Court was partly criticised for its merits, namely because the court did not acknowledge in full that Internet connection might be obtained at significantly lower rates and that the active component of information self-determination does not include a right to have access to cable TV. However, the inclusion of the active component of informational self-determination was accepted by Czech doctrine as one of the possible forms of interpretation of the right to a personal life[48].

47 Decision file number I. ÚS 22/10, N 77/57 SbNU 43, English translation available online at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=372&cHash=1c2ede3ef55d98e9b6f7c2ebd4dc416b.

48 For a doctrinal comment on the decision, see Polčák, R. *Internet a proměny práva*, Praha: Auditorium, 2012, p. 324.

The court held:[49]

> *"The Constitutional Court also ascribed to this concept of the right to a private life, when it stated in its judgment file No. II. ÚS 517/99 that: "[T]he right to protection of personal privacy is the right of a natural person to decide according to his own deliberation whether, or to what extent and in what manner, the facts of his own personal privacy are to be made accessible to other subjects, and at the same time to defend oneself against (resist) unjustified interference in that sphere by other persons. Excessive emphasis on the positive component of the right to protection of one's private life leads to inappropriately narrowing of protection to merely seeing to it that the facts of a person's private life not be [disclosed] without his consent or without reasons recognized by the law, and thus the integrity of the internal sphere, which is essential for positive personal development, not be violated. The Constitutional Court does not share this narrowed understanding, because respect for private life must, to a certain degree, include the right to form and develop relationships with other human beings. Respect for private life, thus understood, includes the commitment of the state to act in a manner that permits the normal development of these relationships" [see judgment file No. II. ÚS 517/99 of 1 March 2000 (N 32/17 SbNU 229)].*
>
> *(…)*
>
> *Therefore, it is the duty of the courts to review the unique aspects of each case so that, apart from observing the guarantees of a fair trial, the individual's other fundamental rights are also preserved - in this case the right to a private life [G. Dürig (G. D., Der Grundrechtssatz von der Menschenwürde, Archiv des öffentlichen Rechts 81, 1956, p. 127) formulated the well-known theory of the object, which was adopted in the case law of the German Constitutional Court, connected to the questions of human dignity. According to this theory human dignity is violated when state authority places a specific individual into the role of an object, in which they become a mere means to an end, and are reduced to a fungible value. One can conclude that a person is not only the object of social "relationships", but also becomes the object of the law, if they are forced to subject to it completely in its interpretation and application, i.e. without taking into account their individual interests, or fundamental rights]. In addition to the subjective factors on the part of the individual, when evaluating whether expenses are "usual or justified", it is also necessary to take into account objective factors, which include, among*

[49] Decision file number I. ÚS 22/10, N 77/57 SbNU 43, English translation available online at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=372&cHash=1c2ede3ef55d98e9b6f7c2ebd4dc416b.

other things, technological developments (e.g. mobile phones, the Internet) and changes in the methods of communication, obtaining information, contact with government offices, association, etc., or the development of technologies, through which the individual's right to personal development, relationship with other people and the outside world, i.e. the right to a private life, is realized (point 17).

The active component of informational self-determination needs to be distinguished from freedom of speech, which covers the right to actively communicate information to the public, i.e. the right to bring one's speech to a public space. On the other hand, the active component of right for informational self-determination (i.e. the right to communicate) includes only those forms of active communication that are regular in individual private (personal) life, including private interpersonal communication, individual requests for information (e.g. by browsing on a website) etc."

2.2 Proportionality of access to data

The doctrine of proportionality has constitutional origins, but it is now also occasionally applied by regular courts and even by administrative authorities. The methodological grounds of proportionality of rights were established in a decision of the Constitutional Court file number Pl. ÚS 4/94. In this case, the court was assessing the constitutional compliance of the institute of anonymous witness and had to find a proportional balance between the witness protection and fair trial rights of the accused.

With respect to proportionate balancing of rights, the Court ruled that: [50]

"When considering the possibilities of restricting a basic right or freedom for the benefit of another basic right or freedom the following conditions can be stipulated governing the priority of one basic right or freedom:

The first condition is their mutual comparison, the other is the requirement to examine the substance and the sense of the fundamental right or freedom being restricted (Art. 4 para 4 of the Charter of Fundamental Rights and Freedoms1).

The mutual comparison of colliding fundamental rights and freedoms is based upon the following criteria:

50 Decision file number Pl. ÚS 4/94, 214/1994 Sb., N 46/2 SbNU 57, English translation available at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=611&cHash=f69da5fcba1a2e433d74385371b3a196.

The first is the criterion of applicability, i.e. a reply to the question whether the institute restricting a certain basic right allows the achievement of the desirable aim (the protection of another basic right). In the given case the legislator can be affirmed in that the institute of anonymous witness allows to achieve the aim, i.e. to guarantee the inviolability of his person.

The second criterion for measuring basic rights and freedoms is the criterion of necessity residing in the comparison of the legislative means restricting some basic right or freedom with other provisions allowing to achieve the same objective, however, without impinging upon fundamental rights and freedoms. The reply to the fulfilment of the criterion of necessity in the second case is not unambiguous: in addition to the legislative construction allowing the anonymity of the witness the government can use also other means for his protection (such as the utilization of anonymous testimony as a criminalistic means for further examination, offering protection to the witness etc.).

The third criterion is the comparison of the importance of both conflicting basic rights. In the case under consideration one of them is the right of fair trial ensuring the right for personal freedom, the other is the right of personal inviolability. These basic rights are prima facie equal.

The comparison of the importance of colliding basic rights (after having fulfilled the condition of appropriateness and necessity) resides in weighting empirical, systemic, contextual and value oriented arguments. As an empirical argument the factual seriousness of a phenomenon can be understood that is connected with the protection of certain fundamental right (in the case under consideration this is the increasing number of cases of threatening and terrorising of witnesses by organized crime). A systemic argument means considering the sense and the classification of the respective fundamental right or freedom within the system of basic rights and freedoms (the right to fair trial in this connection is part of the general institutional protection of basic rights and freedoms). As contextual argument also further adverse impacts of the restriction of one fundamental right due to the favouring another right can be understood (in the given case the possibility of misusing the institute of anonymous witness in the criminal procedure). The value argument represents considering the positive aspects of the conflicting fundamental rights as regards the accepted hierarchy of values.

Part of comparing the relative weight of the conflicting basic rights is also considering the utilization of legal institutes minimizing the intervention into one of them, supported by arguments."

As a result, the Court has established a three-step test, which consist of the following parts:

- Suitability – a question as to whether the respective limitation of a fundamental right is able to serve the desired purpose.
- Necessity – a question as to whether there might not be some other alternative ways to achieve the desired effect without a need to limit the respective fundamental right(s)
- Proportionality stricto sensu – a question as to whether there is a reason for an ad hoc preference of one fundamental right over another.

If some limitation of a fundamental right passes the test outlined above, there must be an additional assessment of whether the fundamental right evaluated as less relevant will be limited only to a necessary extent. This assessment, known also as the limited proportionality test, is in many cases crucial. For example, in the case of data retention[51] or access to retained data[52], the respective limitations of privacy passed all three tests. That means that the Court stated that these measures were fit for the purpose, there were no reasonable alternatives and that there was a good reason to prefer certain fundamental rights over privacy. However, the Court held that the way in which data retention was legislated into the statutory law lead to a greater impact on privacy than necessary. In other words, the Constitutional Court has regularly struck down instruments, which were proportionate per se, but had to be legislated using less intrusive measures or implementing more safeguards and balances.

In the case No. Pl. ÚS 24/11, in which the Court assessed simple statutory provisions empowering law enforcement and security authorities to request traffic and geolocation data, the Court ruled (official translation): [53]

"27. In a democratic society, apart from expressing the requirement of necessity,

51 See Decision of the Constitutional Court file number Pl.ÚS 24/10. For a detailed analysis of constitutional developments regarding data retention in the Czech Republic, Myška, M. *Právní aspekty uchovávání provozních a lokalizačních údajů*, Brno: Masarykova univerzita, 2013, 133 s.

52 See Decision of the Constitutional Court file number Pl. ÚS 24/11, 43/2012 Sb., N 217/63 SbNU 483, English translation available at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Decisions/pdf/Pl_US_24-11.pdf.

53 See Decision of the Constitutional Court file number Pl. ÚS 24/11, 43/2012 Sb., N 217/63 SbNU 483, English translation available at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Decisions/pdf/Pl_US_24-11.pdf.

the contested legal regulation should also contain the manner of handling the data on the side of the bodies active in criminal proceedings. It should include unambiguous and detailed rules containing the minimum requirements concerning the security of the retained data, which would guarantee that they will not be used for any other purposes than those stipulated by law. In particular, this involves restricting third-party access and defining the procedure of maintaining data integrity and credibility, or the removal procedure (the Judgment file reference Pl. ÚS 24/10, paragraph 50). Efficient protection against the unlawful interference with the fundamental rights and freedoms of the affected individuals should be guaranteed by means of a duty to subsequently inform the user of the electronic communication services, provided that the person's identity is known, and that the traffic and location data concerning this person have been disclosed to the bodies active in criminal proceedings. At the same time, the person should be provided with a legal means on the basis of which they could seek judicial review of the procedure of collecting and handling the relevant data. Any exemption to this duty would be admissible only for the reasons stipulated by law, where the interest in concealing the information prevails. Yet even in these cases, the legislature must guarantee that the assessment of the relevant authorities as to whether there are grounds for concealing the information was not arbitrary but was subject to obligatory judicial review (cf. also similar conclusions contained in the Judgment of the Federal Constitutional Court of Germany issued on 2 March 2010, file reference 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, especially paragraphs 281 and 282). In this respect, the Constitutional Court adds that there is no reason why the extent of the guarantees stipulated by law in relation to ordering the disclosure of the telecommunication traffic data should differ from the perspective of its content, unless such distinction is of essential character, from the guarantees stipulated in relation to ordering telecommunication traffic interception and records, without regard to the existing legal regulation, since in both cases the intensity of the interference with the right to privacy is comparable."

As can be also noted from the above citation, the Czech constitutional doctrine of proportionality is to a large extent inspired by the German constitutional practice as well as by the works of German legal scholars.[54] Consequently, fundamental rights are all methodologically treated

54 The doctrine of proportionality of fundamental rights is directly derived from Rober Alexy's method of assessment of contradictory legal principles – see Alexy, R. Constitutional Rights, Balancing and Rationality, 2003, *Ratio Iuris*, Vol. 16, No. 2, 131-140.

by the Court as legal principles, which means that none of them is superior to another per se (their mutual relations always have to be resolved ad hoc). Thus, it is impossible to state that for instance privacy is in general more relevant for the Court than freedom of speech – on the contrary, every conflict of fundamental rights (or in general of any constitutional principles) has to be assessed on a case-by-case basis.

2.2.1 Secrecy of telecommunications

The doctrine of proportionality was used in a number of cases, namely with regards to wiretapping. In most cases, the courts (namely the Supreme Court and the Constitutional Court) did not assess the mere question as to whether wiretapping is compliant with the proportionate understanding of constitutional rights, but rather reviewed only the form in which wiretapping was used in a particular case, including its procedural aspects. That means that wiretapping is not normally subject to full review as to its mere existence in the Czech judicial practice, but rather as to the form in which it is used in particular cases.[55]

A specific issue, also considered by the Constitutional Court in several cases, is the transferability of wiretapped records. In this issue, the Court had to deal namely with subjective and substantive transfers. Substantive transfers are such transfers that happen e.g. when the Police has received a court order for wiretapping reasoned by a particular suspicion of a crime and later it is determined that it might be used as an evidence in a different criminal matter (e.g. the court order is obtained for the crime of fraud and it turns out later that the wiretapped data can be used as crucial evidence in a case of blackmail). In these cases, the Constitutional Court has regularly ruled in favour of such use of wiretapped data.[56]

On the other hand, subjective transfers are such transfers that happen not just upon different causes but among different institutions. It means that e.g. the domestic intelligence agency received a court order for intelligence purposes and it then turned out the data could be used by the Police in an investigation

55 For detailed analysis of constitutional cases related to wiretapping and use of wiretapped data, see for example Pokorný, L. *Zpravodajské služby*, Praha: Auditorium, 2012.

56 See for example Kybic, P. K otázce použití odposlechu a záznamu telekomunikačního provozu jako důkazu v jiné trestní věci, *Trestněprávní revue*, 2002, Vol. 1, No. 4, p. 114–117.

of a crime. In such cases, the Constitutional Court has regularly ruled against the admissibility of such evidence in criminal trials, since it has ruled that once the eventuality of possible use of wiretapped data by a different institution arises, such an institution is obliged to request a new order.[57]

2.2.2 Secrecy of retained traffic data

In terms of the protection of fundamental rights against state intrusions, the Czech Republic is substantially different from countries that have not been ruled by a Nazi or a Communist regime. Even 25 years after the political changes of 1989, the general assumptions in the society regarding the regular functioning of the state and its security institutions are a priori negative. Even the Supreme Administrative Court and the Constitutional Court present themselves as judicial bodies whose main purpose is to protect the individual against intrusions committed by the state. Consequently, there is a significant level of suspicion about any new forms of state activity, which intrude upon individual constitutional rights.[58]

Unlike some other EU Member States, the Czech Republic had data retention legislated prior to the adoption of the Directive. Upon the adoption of the Directive, the provisions laid down in the Telecommunications Act were broadened and so was the range of state institutions entitled to ask for such data.

A recently applicable version of data retention is valid after the Constitutional Court has ruled against its first implementation. Using the doctrine of proportionality, the Constitutional Court has stated that the retention as such might be fit to fulfil all three steps of the proportionality test, but that it does not meet the requirement of minimum possible intrusion.

The Court ruled that (official translation):[59]

> *"The primary function of the right of respecting private life is to provide space for development and self-realization of the individual personality. Apart from the traditional definition of privacy in its space dimension (protection of the home*

57 See Polčák, R., Púry, F., Harašta, J. et al. *Elektronické důkazy v trestním řízení*, Brno: Masarykova univerzita, 2015, p. 181.

58 See Pokorný, L. *Zpravodajské služby*, Praha: Auditorium, 2012, 150 p.

59 Decision file number Pl. ÚS 24/10, 94/2011 Sb., N 52/60 SbNU 625, English translation available at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=c574142df486769e0b435954fead08c3.

in a broader sense) and, in connection with the autonomous existence and public authority, undisturbed creation of social relationships (in a marriage, family or society), the right to respecting private life also includes the guarantee of self-determination in the sense of primary decision-making of an individual about themselves. In other words, the right to privacy also guarantees the right of an individual to decide, at their own discretion, whether and to what extent, how and under what circumstances the facts and information concerning their personal privacy should be made accessible to other entities. This aspect of the right to privacy takes the form of the right to informational self-determination, expressly guaranteed in Article 10, para. 3 of the Charter.

The right to informational self-determination is thus a necessary condition not only for free development and self-realization of an individual, but also for establishing free and democratic communication rules. Put it simply, under the circumstances of an omniscient and omnipresent state and public authority, the freedom of expression, the right of privacy and the right of the free choice of behaviour and acting become virtually non-existent and illusionary.

Although the prescribed obligation to retain traffic and location data does not apply to the content of individual messages [see Article 1, para. 2 of the Directive 2006/24/EC of the European Parliament and Council of 15 March on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereafter only as the Data Retention Directive) and the contested provisions of Section 97, para. 3, sentence 4) of Law No. 127/2005 Coll. on Electronic Communications and Amendment of Some related Acts (Act on Electronic Communications) in their latest wording] the data on the users, addresses, precise time, dates, places, and forms of telecommunications connection, provided that monitoring takes place over an extended period of time and when combined together, allows compiling detailed information on social or political membership, as well as personal interests, inclinations or weaknesses of individual persons.

On condition that the criminal law allows for exercising the public interest to prosecute criminal activity by means of robust tools the use of which results in serious limitations of the personal integrity and fundamental rights and freedoms of an individual, then when applied, constitutional law limits have to be respected. Restrictions imposed on personal integrity and individual privacy (i.e. breaching the respect towards them) may only be applied as an absolute exception, provided it is deemed necessary in a democratic society, unless it is possible to meet

the purpose pursued by the public interest in any other way and if it is acceptable from the perspective of the legal existence and respecting effective and specific guarantees against arbitrariness. Essential presumptions of a due process require that the individual be provided with sufficient guarantees against the potential abuse of power by the public authorities.

With respect to the seriousness and extent of the infringement of the right to privacy in the form of the right to informational self-determination (in the sense of Article 10, para. 3 and Article 13 of the Charter), represented by the use of the retained data, the legislature limited the possibility to use the retained data only for the purposes of criminal proceedings prosecuting serious crime and only in the case that such an objective cannot be achieved using any other means. In fact, this is anticipated not only by the Data Retention Directive, referred to above, but also by the provisions of Section 88, para. 1 of the Criminal Procedure Code, defining the conditions for enacting interception and records of telecommunications operation ("on condition that criminal proceedings related to serious crime have been initiated"), from which the afore-mentioned legal regulation included in the provisions of Section 88a of the Criminal Procedure Code as a whole deviates without any due reason, providing for the legal regulation in obvious contradiction to the opinions of the Constitutional Court.

As for the examined case of global and preventive collection and retention of data on electronic communications, the need to have such guarantees available is becoming even more important to the individual owing to the current enormous and fast-moving development and occurrence of new and more complex information technologies, systems and communication tools, which unavoidably results in the borders between private and public space being blurred to the benefit of the public sphere, since in the virtual environment of information technologies and electronic communications (in the so-called cyberspace), every single minute, especially owing to the development of the Internet and mobile communications, thousands or even millions of items of data and information are recorded, collected and virtually made accessible, interfering with the private (personality) sphere of the individual, yet if asked, they would probably be reluctant to knowingly let someone else in."

We might speculate that the original draft of the reasoning of this decision might have contained even stronger statements about the actual constitutional disproportionality of the instrument of data retention as such. The final version of the reasoning, however, includes these formulations only in the form of rhetorical questions as a part of its obiter dictum. In any

case, the Court's very strong stance against the form, in which data retention had been previously legislated, is apparent from the fact that the respective provisions of Czech statutory law were repealed with immediate effect (this caused significant problems to law enforcement and security authorities in the time between the publication of the decision and the adoption of new legislation).

In addition to the above-cited decision, the Constitutional Court also ruled against a provision that originally provided for the opportunity of various authorities to request traffic data for the purpose of criminal procedure. In this case, the Court essentially stated that procedural safeguards in requesting of traffic data should be analogically strong as in the case of wiretapping. The Court ruled (official translation):[60]

> *"It may be summarised that although Section 88a of the Criminal Procedure Code contains the complete legal regulation of access to the telecommunication traffic data for the bodies active in criminal proceedings, this access is expressly determined only by stipulating that the relevant data may only be identified for the purposes of clarification of the circumstances significant for the criminal proceedings. Although the assessment as to whether this condition has been met is granted to the presiding judge or the judge within the preliminary proceedings, who decides on ordering such data, its very general and vague definition cannot be deemed sufficient. That is especially true when taking into account the absence of any further regulation concerning the subsequent disposal of the data and the fact that disclosing the data in question represents, in relation to the affected users of electronic communications services, an interference with their fundamental right to privacy in the form of the right to informational self-determination pursuant to Art. 10, para. 3 and Art. 13 of the Charter and Art. 8 of the Convention. Above all, the legislature utterly failed to reflect the requirement of proportionality of interference with fundamental rights with respect to the pursued goal in the contested provision, since the access to the data in question is authorised, in essence, as a common means of collecting evidence for the purposes of criminal proceedings, conducted for any criminal offence whatsoever. In view of the seriousness of the relevant interference with an individual's private sphere, this limitation will only pass the test if it meets the conditions arising from the proportionality*

60 Decision of the Constitutional Court file number Pl. ÚS 24/11, 43/2012 Sb., N 217/63 SbNU 483, English translation available at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Decisions/pdf/Pl_US_24-11.pdf.

principle. That means that the access of the bodies active in criminal proceedings to the telecommunications traffic data may only come into question when the purpose of the criminal proceedings cannot be achieved any other way. The legal regulation must therefore contain sufficient guarantees for preventing the use of such data for any other purposes than those assumed by the law and that the restriction of the individual's right to informational self-determination does not amount to excessive interference with respect to the importance of specific societal relationships, interests or values that are subject to the criminal offence subject to the corresponding criminal proceedings. The contested provision does not respect these limitations and this deficiency may not be eliminated even by means of the stipulated judicial review. In their decisions on ordering the disclosure of relevant data, courts may grant protection to the right to informational self-determination with respect to the facts of a particular case, yet their case law cannot replace the absence of a sufficient, definite and legitimate legal regulation, which is, pursuant to Art. 4, para. 2 of the Charter, a condition for placing limitations upon fundamental rights and freedoms in general."

In comparison with the case of substantive statutory provisions, which lay down merely the data retention obligations, the Constitutional Court did not consider the procedural constitutional disproportionalities, although they were found unconstitutional, as equally problematic. We might also speculate that the Court may have noted the serious problems previously caused by the immediate effect of its prior decision on data retention. Consequently, Article 88a of the Code of Criminal Procedure was repealed with a sufficient delay to enable the adoption of a constitutionally compliant alternative.

The Court also expressly stated that although the statutory procedure was unconstitutional as such, it did not imply a lack of constitutional compliance (and the subsequent inadmissibility of the retained data as evidence) in individual criminal cases per se. Although some of the accused or sentenced individuals later tried to challenge the admissibility of such evidence in their trials, the results were mostly in favour of admissibility. In that respect, we might state that the lack of proportionality in the substantive and procedural statutory rules of data retention was in practice often cured by the fact that the respective Police forces, State Prosecutors etc. acted

in a manner that is constitutionally compliant. In other words, the Police or Public Prosecution acted in certain cases with a higher standard of protection of individual rights than what was expressly demanded by the applicable law.

2.2.3 Secrecy of information systems

For a relatively long time, the Czech law did not include any instrument making intrusions into information systems illegal as such. Criminal law, as well as civil and administrative law included specific provisions that made it possible to sanction destructive intrusions (e.g. those that lead to damaging these systems or revealing data) or intrusions made against specific kinds of systems (e.g. systems containing classified data).[61] However, an intrusion in itself was not subject to any specific kind of legal sanctions.[62]

Nowadays, the Czech criminal law contains different provisions, which ensure for criminal liability in cases of simple intrusions. Consequently, it is possible to prosecute an offender only upon proving the mere fact of intrusion (i.e. without the need to prove actual damage).[63]

Section 232 of the Criminal Code provides for criminal sanctions only in cases when damage to data is proven. That is analogous to the aforementioned provision of repealed Criminal Code that originally served the purpose of protecting information systems against intrusions.

Including criminal sanctions for a mere intrusion of information systems triggered negative response mainly from computer scientists.[64] There was even a popular petition against the adoption of new types of criminal conducts into the Criminal Code, motivated by the fear that freedom of scientific research was being threatened (research and development in computer

61 For a historical overview of the development of the Czech cybercrime law, see Smejkal, V. *Kybernetická kriminalita*, Plzeň: Aleš Čeněk, 2015, 636 p.

62 See Smejkal, V. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku, *Trestněprávní revue*, 2013, Vol. 2, No. 6, pp. 161-166.

63 See sections 182, 183 and 230 – 232 of the Criminal Code. For detailed description, see Šámal, P. et al. *Trestní zákoník – komentář II. § 140-421*, Praha: C. H. Beck, 2009, pp. v-xiv, 1451-3586.

64 See for example the public petition titled „Opinion of IT Security Experts on the Clarification of the Amendment to the Criminal Code" (Názor odborníků z oblasti ochrany informačních systémů k upřesnění návrhu trestního zákoníku), published online 11. 10. 2015 at http://itpravo.cz/index.shtml?x=694071.

sciences includes, namely as to security assignments, the possession and use of intrusive tools, which fall under the hypotheses of the above-cited provisions). The Criminal Code, however, contains an escape clause (called 'material corrective' in the Czech doctrine of criminal law), which makes it possible to prosecute only such conduct that is harmful to society. This requirement is laid down, together with the principle ultima ratio, in section 12, para 2, which reads as follows: *"Criminal liability of an offender and criminal consequences associated with it may only be applied in socially harmful cases where application of liability according to other legal regulations does not suffice."*

2.3 Statutory consequences of constitutional protection

Historically, intrusive measures, as well as protective instruments, were primarily focused on real-time communications and specifically on telecommunications (nowadays called 'electronic communications'). Consequently, there is, apart from the Charter of Fundamental Rights and Freedoms cited supra, also a set of more or less traditional black-letter rules that lay down in detail the procedures for wiretapping and the subsequent use of acquired data.

On the contrary, the Czech law does not have much regulatory experience with stored communications, i.e. with data that are for some reason stored somewhere and can also be used as evidence or as security intelligence. The only examples of relatively detailed rules that are related to stored communications are those implemented for the retention of traffic data.[65] In any case, there is still a lack of more detailed provisions for communications (data) stored on personal devices and those stored by providers of information society services, apart from electronic communications service providers.

For example, the acquisition and forensic analysis of mobile communication devices is subject to the same rules as acquisition of any other tangible assets.[66] Similarly to that, there are no specific rules for the Police

65 For a detailed analysis of these provisions, see Chudomelová, Z., Beran, M., Jadrný, V., Němečková, Š., Novák, J. *Zákon o elektronických komunikacích – komentář*, Praha: Wolters Kluwer, p. 313.

66 See for example Polčák, R. Púry, F., Harašta, J. et al. *Elektronické důkazy v trestním řízení*, Brno: Masarykova univerzita, 2015, p. 121 and 145.

or other forces with investigative powers to request data that are stored, mostly upon the consent of users, by providers of hosting services,[67] which fall outside the licensing regulations for providers of services of electronic communications.[68]

All that, of course, does not mean that the Police or the Prosecution Service would be entirely disqualified from working with stored e-mails or files in the clouds – in such cases, they just have to apply the general rules originally made with an entirely different teleology. Apart from the lack of efficiency, redundant formalities and sometimes even the lack of logical sense (in some areas, the Police uses, in order to get stored data, the terms related to stored tangible assets), another problem is that this situation might also lead to a higher risk of ad hoc disproportionate infringement of constitutional rights. It is, in our view, only a matter of time before the courts start ruling against the admissibility of evidence obtained from some stored communications, simply due to the fact that the general procedural tools used to acquire it did not provide for enough safeguards as to informational self-determination or other individual (distributive) informational rights.

2.3.1 Protection of the secrecy of telecommunications

Apart the Charter of Fundamental Rights and Freedoms (cited supra, II.2.1), the secrecy of telecommunications is protected by a number of statutory provisions. In particular, the Electronic Communications Act contains specific provisions which lay down in relatively detailed manner the duties of electronic communications service providers to secure substantive data (content), traffic data and related metadata (e.g. directories) from unlawful interference.[69] In any case, the aforementioned provisions, whenever they apply on personal data, act as lex specialis in relation to the Personal

67 See Art. 14 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

68 Stored data discovery and acquisition is, together with freezing orders, currently dealt with by a special expert group of the Ministry of Justice, which aims to draft an amendment to the Code of Criminal Procedure specifically for that purpose. This initiative, however, has proven, for various reasons, to be more complex and problematic than it was originally envisaged.

69 See Chudomelová, Z., Beran, M., Jadrný, V., Němečková, Š., Novák, J. *Zákon o elektronických komunikacích – komentář*, Praha: Wolters Kluwer, p. 289.

Data Protection Act.[70] Any subsequent forms of processing of personal data, including the rights of data subjects, the limitations regarding transfers of data to other jurisdictions, etc. are regulated by the Personal Data Protection Act. The subsequent applicability of the Personal Data Protection Act became apparent in a case where a user requested traffic data from the operator of their mobile phone. That request was based on a general provision of the Personal Data Protection Act, which lays down in the section 12 the duty of a controller to inform the data subject, upon a request, about any of their personal data that are being processed.[71]

It is to be noted that general provisions of the data protection law apply, apart providers of services of electronic communications, also to other information society providers (e.g. on-line messengers, hosting providers etc.). However, these providers are not recognised as electronic communications providers by Czech law, so we do not deal with their obligations.

2.3.2 Protection of the confidentiality and integrity of information systems

The issues of confidentiality and integrity of information systems (and eventually of the third aspect of IT security, i.e. the availability) are not recognised in the form of a specific constitutional principle. As noted above, they are constitutionally protected through the protection of the respective systems as such (namely by the general protection of property) or by the protection of data stored therein (i.e. by the protection of information self-determination, the freedom of speech, the freedom of scientific research, the right to work etc.)

Confidentiality and integrity, however, form a specific part of the Czech law of electronic communications.

Sections 98 and 99 of the Electronic Communications Act cover the providers of services of electronic communications.[72] Apart from that,

70 Act No. 101/2000 Sb., English translation available at https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1107.

71 For a detailed analysis of specific provisions of the Czech Data Protection Act, see Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D. *Zákon o ochraně osobních údajů – komentář*, Praha: C. H. Beck, 2012.

72 In detail, see Chudomelová, Z., Beran, M., Jadrný, V., Němečková, Š., Novák, J. *Zákon o elektronických komunikacích – komentář*, Praha: Wolters Kluwer, p. 325.

the confidentiality and integrity of information systems and information networks is also subject to the Cybersecurity Act[73], which defines its main aim, i.e. the security of information in section 2 c) as follows (informal translation): "Security of information means ensuring the confidentiality, integrity and availability of information".

Under normal circumstances, the Cybersecurity Act applies to administrators of information and communication systems, which belong to specifically listed critical information infrastructure, administrators of important information systems (specifically listed public information systems) and administrators of important networks (i.e. networks with direct cross-border connectivity). These entities are, regardless of their nature (i.e. private or public entities), obliged to implement standard security measures and to report in real-time the occurrence of cybersecurity incidents to a national or governmental CERT. They also have to obey administrative orders issued by the National Security Authority (Narodni bezpecnostni urad). Any lack of compliance is, just like in the case of the Electronic Communication Act, considered an administrative offence.[74]

2.3.3 Protection of the core area of privacy

The only part of the Czech law where privacy stricto sensu is addressed specifically is private law. However, the Civil Code, although adopted as recently as 2012, reflects neither the recently problematic nature of the concept of privacy nor its current technological determination. The reason is that its structure and wording is hugely inspired mostly by Code Civil, ABGB, BGB and by Czech legislative drafts from the first half of the twentieth century. As a result, the Czech Civil Code includes only very general provisions whose meaning for the everyday life in the information society is highly uncertain.

Moreover, the Civil Code introduces an extremely broad concept of an asset (věc) – anything (including rights) "distinguished from an individual and

73 Act No. 181/2014 Sb., English translation available at https://www.govcert.cz/download/nodeid-1143/.

74 For a complex overview of Czech cybersecurity law, see Polčák, R. Kybernetická bezpečnost jako fenomén českého práva, *Revue pro právo a technologie*, 2015, Vol. 6, No. 11, p. 95-149.

useful to humans" is considered to be an asset. The implementation of this traditional Austro-German concept into the Czech law was entirely new and so there is a substantial shortage of case-law that would clarify even the basic interpretative questions. In particular, it is questionable whether personal data or other data that originate in the private information sphere of an individual, might be considered "assets." On one hand, they can be distinguished from individuals (they can exist independently); on the other hand, they are still strictly related to them. A similar situation exists in the case of profiles on user-generated-content services processing personal data (e.g. social networks).[75]

The relative uncertainty of the meaning of privacy stricto sensu in private law leads to practically problematic situations where even very basic disputes have to be handled as hard cases. In such cases, even regular courts have to apply the doctrine of proportionality described in the first part of this chapter. For example, the Regional Court of Brno had to decide a case, in which an owner of an apartment building installed cameras into the entrance hall and justified their presence by the purpose to protect mailboxes from theft. The court applied the full proportionality test and held that such an installation is not proportionate, as there are less privacy-intrusive alternatives available for achieving the same purpose (i.e. to preventively protect mailboxes).[76]

The relatively vague nature of the meaning of the term 'privacy' in the Czech law (whether it be constitutional or private law) means that the concept of privacy is not used in administrative or criminal law. In particular, the liability for administrative offences and crimes is constructed upon more formally defined terms like "personal data," "traffic data," "correspondence" etc.

2.3.4 Criminal liability for the unlawful infringement of the telecommunication secrecy

The Criminal Code offers several of options that cover different possibilities of unlawful interference with communication networks. The Czech Republic is party to the Budapest Treaty,[77] so these provisions reflect the standard

75 For a detailed discussion of this issue, see Polčák, R. Informace a data v právu, *Revue pro právo a technologie*, 2016, Vol. 7, No. 13, pp. 67-91.

76 See case No. C 45/2007-121 (Krajský soud v Brně, 6 November 2015).

77 The treaty was finally passed and promulgated in 2013 under No. 104/2013 Sb.m.s.

types of crimes laid down therein.[78] In particular, unlawful interference can be typically subsumed under the following:

- section 182 Violating Confidentiality of Messages;
- section 230 Unauthorised Access to Computer Systems and Information Media.

It ought to be noted that there are specific provisions in the Electronic Communications Act and Cybersecurity Act, which lay down technical requirements for the providers of various telecommunication services. As a result, there is a reason to expect that such services are properly technically secured and any unlawful interference would require overcoming some security measures. Thus, it is possible to sanction the unlawful interference also through the possession crime aimed at devices and tools (including passwords) whose aim it is to access protected systems or networks – in particular, the Criminal Code provides for section 231 Measures and Possession of Access Devices and Computer System Passwords and other such Data.

It must be noted that the Czech criminal law sanctions also preparatory activities as well as attempted crimes, as laid down in sections 20 and 21 of the Criminal Code.

Stored communications are protected by the criminal law through the crime defined in section 183 as Breach of Confidentiality of Documents and other Privately Kept Documents. Subsequently, it is also possible to use section 230 Unauthorised Access to Computer Systems and Information Media and section 231 Measures and Possession of Access Devices and Computer System Passwords and other such Data.

In any case, it is relatively complicated to formulate doctrinal opinions about particular elements of the aforementioned protective provisions, as relevant case-law is still not available. For example, there are no cases so far that would provide for answers as to the applicability of section 230 or section 231 in relation to decryption keys or other tools making it possible to work with encrypted data.

78 For a discussion of the implementation issues of the Budapest treaty, see for example Smejkal, V. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku, *Trestněprávní revue*, 2013, Vol. 2, No. 6, pp. 161-166.

2.3.5 Protection of professional secrets in criminal procedural law

The Czech law does not have a common denominator for professional secrets. However, certain sorts of data are specifically protected in criminal procedural law through the general protection of secrecy and protection of classified information. Duties of secrecy are contained in different parts of Czech statutory law. The most important examples for the scope of this book include the duties of secrecy laid down in the Advocacy Act,[79] those defined in medical law (secrecy of health records), banking law (secrecy of bank account data), those defined in the Electronic Communications Act or those laid down in the Cybersecurity Act (secrecy of records on cybersecurity incidents). A very specific case relates to the secrecy duties with regards to security files, i.e. personal files assembled by the National Security Authority in the course of evaluation of applicants for a security clearance (i.e. for the permission to handle classified information) – there are only extremely exceptional cases when, together with client data held by solicitors, these data might be used in criminal proceedings. In the case of other sorts of data covered by secrecy duties, the respective statutory provisions always contain relatively accessible procedures for the exclusion of secrecy duties.

The main provision covering the use of data under secrecy duties is contained in section 8 of the Code of Criminal Procedure. The provision implies that the most sensitive sort of data covered by secrecy duties are the client's data, processed by their solicitor. The higher level of their statutory protection is based on the right to a fair trial, which also includes the right for professional representation at court. Such representation can be provided only if the client is able to give their solicitor open access to the complete data about their case (incl. information that might not be favourable to their court standing). Consequently, such data have to be excluded from being available to the prosecutors or the police. Therefore, when the data processed by solicitors are to be gathered and used in criminal proceedings, a special procedure involving the Bar association and a court decision is required.

The so-called 'advocate confidentiality,' is, as to its range and possibilities of abuse, subject to a continuous debate in the Czech Republic. On the one

79 Act No. 85/1996 Sb., English translation is available at http://www.cak.cz/assets/act-on-legal-profession_219_2009.pdf.

hand, solicitors tend to abuse this statutory limitation to cover corruption, money laundering, operations prohibited by antitrust laws etc.[80] On the other hand, the Public Prosecution Service is constantly testing the boundaries of this statutory protection and so raids on stored solicitor communications are not rare.

Recently, there a decision was made in a highly debated case, in which the Public Prosecution Service requested a permission to search a cloud storage facility that contained solicitor communications.[81] The law firm in question refused to provide the requested data with a reference to the aforementioned 'advocate confidentiality'. The Public Prosecution Service requested a court warrant and the court held that data stored in cloud, i.e. outside of premises of the solicitor, should not be regarded as client-solicitor communication – meaning that solicitors are obliged to keep such data under their physical control. The court therefore considered the storage on a cloud service as proof of the fact that these data are not to be regarded as solicitor-client communication.

This decision triggered strong reactions from the Bar Association and its members, because it can be technically interpreted in the sense that protection under the header of 'advocate confidentiality' only applied to such data that are physically stored within the premises of the respective solicitors. This would technically ban solicitors from using cloud services (even those based on specifically rented secure servers). However, the reasoning of the decision in question did not provide sufficient technical detail as to the conditions under which the seizure of solicitor data in the cloud was possible, so there is a reason to expect further development of the Czech case law in this matter.[82]

---

80 This was mentioned even in a decision of the Constitutional Court file number III. ÚS 3988/13, U 5/72 SbNU 583, available in Czech (no known English translations are available to this date) at http://nalus.usoud.cz/Search/ResultDetail.aspx?id=83083&pos=1&cnt=1&typ=result.

81 Interim decision (usneseni) No. Nt 615/2014, available in Czech (no known English translations are available to this date) at http://www.scribd.com/doc/235322741/Nt-615-2014.

82 See for example Smejkal, V. Ochrana dat advokátů v elektronických úložištích, *Bulletin advokacie*, 2015, No. 3, pp. 15-22.

2.3.6 The principle of the "purpose limitation of personal data"

The principle of the purpose limitation of personal data is incorporated in the Personal Data Protection Act. The most important provisions that lay down the purpose limitation are section 5 paragraphs 1 and 2. These provisions are general and apply to all kinds of personal data, including data processed by providers of electronic communications services, services of information society etc. The general purpose limitation, however, does not apply on security, defence and law enforcement bodies, as these are exempt by section 3 para 6, whichreads as follows:[83]

> *"The provisions of Article 5(1) and Articles 11 and 12 of this Act shall not apply to processing of personal data necessary to fulfil obligations of the controller provided by special Acts to ensure:*
> *(a) security of the Czech Republic,*
> *(b) defence of the Czech Republic,*
> *(c) public order and internal security,*
> *(d) prevention, investigation, detection and prosecution of criminal offences,*
> *(e) important economic interest of the Czech Republic or of the European Union,*
> *(f) important financial interest of the Czech Republic or of the European Union, in particular the stability of financial market and currency, functioning of currency circulation and system of payments as well as budgetary and taxation measures, or (g) exercise of control, supervision, surveillance and regulation related to exercise of public authority in the cases under (c), (d), (e) and (f), or (h) activities related to disclosure of files of the former State Security."*

The exemption of the aforementioned authorities and public bodies from the general purpose limitation does not mean that the purpose limitation does not apply at all. Such processing is also limited by its purpose, because the Act expressly states that the processing powers are to ensure (i.e. for the purpose of) security, defence etc. The respective state authorities and other bodies are then limited as to the scope and methods of processing of personal data by statutes that specifically define their powers. All such authorities are then internally and externally supervised, so the purpose limitation applies not directly through the Personal Data Protection Act

83 For a doctrinal commentary, see Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D. *Zákon o ochraně osobních údajů – komentář*, Praha: C. H. Beck, 2012, p. 12.

but through regular limitations and supervisory powers over their activities. It is also to be noted that a general constitutional principle applies, regarding the fact that state institutions may only engage in operations that are expressly ordered or permitted by the law – this principle is laid down in Article 2(3) of the Constitution, which reads as follows: "State authority is to serve all citizens and may be asserted only in cases, within the bounds, and in the manner provided for by law."[84]

84 Constitutional Act No. 1/1993 Sb., English translation is available at http://www.psp.cz/en/docs/laws/constitution.html.

3 POWERS FOR ACCESSING TELECOMMUNICATION DATA

3.1 Overview

The key regulation the interception of electronic communication and other methods for accessing electronic communications data for the purpose of criminal investigations, is contained within the Code of Criminal Procedure.[85]

There are two specific provisions of the Code of Criminal Procedure that allow law enforcement authorities to intercept electronic communication and to access electronic communications data for the purpose of criminal investigations – sections 88 and 88a.

The first of these lays down the rules for interception and recording of electronic communications, while the second one states the rules for accessing metadata related to data transmission in electronic communication networks, which are the subject of the telecommunications secret or which are subject to the protection of personal and intermediation data. Section 88 basically allows law enforcement authorities in criminal proceedings to intercept and record the content of data transmissions in real time, under specified conditions, whereas section 88a allows them, under specified conditions, to access traffic and location data, which must be retained by all entities providing a public communications network[86] or a publicly available electronic communications service[87] (ISPs) in accordance with the Act on Electronic Communications.[88]

85 Act No. 141/1961 Sb. on Criminal Procedure.

86 An electronic communications network used fully or mainly for providing publicly available electronic communications services, which support the transfer of information between end nodes of the network. See Section 2 of the Act on electronic communications.

87 A publicly available service normally provided for a remuneration, which consists fully or mainly of a transfer of signals via electronic communications networks. See Section 2 of the Act on electronic communications.

88 Act No. 127/2005 Sb. on electronic communications and amending certain related laws (the Act on Electronic Communications).

Since there are no other specific rules for coercive powers trying to obtain stored data, communications stored by the user or the ISP may be accessed and processed in accordance with more general provisions, which allow law enforcement authorities to obtain (with the subject's consent, or upon request according to Section 78 of the Act on Criminal Procedure) or seize (Section 79 of the Act on Criminal Procedure) devices and storages in which the data are stored, to conduct surveillance of persons and things during (section 158d of the Act on Criminal Procedure) which the data may be gathered, or to request respective information or data using production order (section 8 of the Act on Criminal Procedure).

Czech statutory law also includes other laws that deal with interception or are somehow important for it. Those primarily include Act No. 127/2005 Sb. on electronic communications and its implementing regulations, Act No. 273/2008 Sb. on the Police of the Czech Republic or Act No. 85/1996 Sb. on advocacy. These acts will be described in more detail bellow.

3.2 Requirement of (reasonable) clarity for powers in the law of criminal procedure

As noted above, the Czech Republic has a relatively long experience with situations when the work of state authorities, including those involved in criminal proceedings, had almost no other purpose than to oppress citizens of a dissenting political opinion. Consequently, the recently applicable limitations on the powers of institutions involved in the criminal procedure are strict and there is also a general tendency to outline these powers quite strictly and precisely. A basic summary of the principles that govern Czech criminal procedural law is provided in Section 2 of the Code of Criminal Procedure.

The need for a strict clarity of powers was also one of the main reasons why the Constitutional Court stopped the previous implementation of data retention obligations, since it contained only general formulations instead of an explicit list of institutions entitled to ask for retained traffic data and

a precise specification of the related procedures, including an explicit possibility for a judicial review. The Court ruled:[89]

> *"37. In its judgments, the conditions outlined above have been specified by the Constitutional Court when assessing the admissibility of the intervention of the public authority to individual privacy taking the form of telecommunication operation interception [cf. e.g. the quoted Judgments file reference II. ÚS 502/2000, file reference IV. ÚS 78/01, file reference I. ÚS 191/05, or file reference I. ÚS 3038/07 issued on 29 February 2008 (N 46/48 SbNU 549)]. The infringement of the individual's fundamental right to privacy in the form of the right to informational self-determination in the sense of Article 10, para. 3 and Article 13 of the Charter, due to the prevention of and protection against criminal activity is thus possible only by means of imperative legal regulations which have to conform to, above all, the rights arising from the principle of the legal state (rule of law state) and which meet the requirements arising from the proportionality test when, in the case of a conflict between the fundamental rights and freedoms with the public interest or any other fundamental rights and freedoms, the purpose (objective) of such infringement must be assessed in relation to the means applied, whereas it is the proportionality principle (in a broader sense) that provides the standard for such assessment. The wording of such legal regulations must be precise and unambiguous, while also being sufficiently predictable so that it provides potentially affected individuals with sufficient information on the circumstances and conditions under which the public authority is entitled to interfere with their privacy and so that they can act accordingly in order to avoid conflict with the restricting norm. Moreover, the powers granted to the relevant authorities, as well as the manner and the rules of application, must be strictly defined so that individuals are provided with protection against arbitrary infringements. From the perspective of the proportionality principle (in a broader sense), assessing the admissibility of the infringement in question includes three criteria. The first one lies in assessing the eligibility of fulfilling the purpose (or appropriateness as well), where it is determined whether the specific measure itself is capable of achieving the intended purpose, being the protection of another fundamental right or public interest. The second criterion consists in assessing the necessity, i.e. examining whether, upon selecting the appropriate means, the one being most*

89 Decision of the Constitutional Court file number Pl. ÚS 24/10, 94/2011 Sb., N 52/60 SbNU 625, English translation available at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=c574142df486769e0b435954fead08c3.

considerate of the fundamental right has been opted for. And finally, it is necessary to assess the adequacy (in a narrower sense), i.e. whether the prejudice to the fundamental right is not disproportionate in relation to the intended purpose, which means that the measures imposing a restriction on fundamental rights and freedoms must not, in case of a collision of the fundamental right or freedom with public interest, exceed (through their negative consequences) the positive aspects represented by the public interest in these measures. [cf. the Judgment file reference Pl. ÚS 3/02 issued on 13 August 2002 (N 105/27 SbNU 177; 405/2002 Sb.)].

(…)

51. Under no circumstances may the stipulation of the duty imposed on legal entities or natural persons to secure that "the content of message should not be retained together with the defined data" (Section 97, para. 3, sentence four) or the duty to "eliminate them upon the expiration of the period unless they have been provided to the competent authorities in compliance with a special legal regulation or unless stated otherwise within the Act (Section 90)" (Section 97, para. 3, sentence six) be deemed by the Constitutional Court as providing sufficient, unambiguous, detailed and appropriated guarantees. The retention period itself, "no shorter than 6 months and longer than 12 months", the expiration of which determines the obligation to remove the data, can also be deemed as ambiguous and totally insufficient with respect to the extent and sensitivity of the retained data. None of these obligations is provided, in more detail, with the rules and specific procedures for how to meet them; the requirements concerning the security of the retained data have not been defined in a stringent manner; it is not sufficiently clear how the data are handled, either by legal entities or natural persons collecting and retaining the location and traffic data, or by the competent public authorities when requested; and the manner in which the data are removed has not been specifically determined either. Similarly, the liability or possible sanctions for failure to comply with such duties, including the absence of the possibility for the individuals affected to seek efficient protection against potential misuse, arbitrariness or failure to comply with the relevant duties have not been defined either. Supervision provided by the Office for Personal Data Protection, as anticipated in the Electronic Communications Act (Section 87 and further), "over observing the duties and obligations when processing personal data" or the corresponding instruments of its activities and monitoring cannot be considered as an adequate and effective means of protecting the fundamental rights of the individuals affected, since they do not control the instrument by themselves [see the Judgment

> *file reference Pl. ÚS 15/01 issued on 31 October 2001 (N 164/24 SbNU 201; 424/2001 Coll.) where appropriate]. As a consequence, the actions referred to above, constituting an obvious infringement of the fundamental right to privacy in the form of the right to informational self-determination (in the sense of Article 10, para. 3 and Article 13 of the Charter) and due to the legal regulation being considered as insufficient and failing to meet the afore-mentioned constitutional requirements, occur beyond the scope or reach of any immediate (yet subsequent) review, particularly a judicial one, the necessity of which has also been expressed by the ECHR in the Decision concerning the case of Camenzind v. Switzerland, referred to above."*

It is to be noted that the Public Prosecution Service and the Police implemented relatively strict procedures internally, which ensured for a precise, case-by-case documentation of each request. They also included court orders (although that not been legislated). Consequently, the retained data used in some previous cases did not have to be declared inadmissible evidence.

The lack of clarity was also the main reason for the Constitutional Court decision cited supra, which repealed the former provisions of the Code of Criminal Procedure that laid down the competence of the Public Prosecution to request retained data. In that case, the Court ruled:[90]

> *"24. The wording of the contested provision implies that the order for disclosure of the telecommunication traffic data is only expressly conditioned by the fact that such measures must pursue the goal of "clarification of the circumstances significant for criminal proceedings". The Constitutional Court believes that the limits of the fundamental right to informational self determination regulated in this manner are formulated too widely and vaguely, and in essence, they allow the relevant data to be requested and used by the bodies active in criminal proceedings each time a certain connection with the on-going criminal proceedings may be associated with them. At the same time, the Court is aware of the obligation of public authorities to apply sub-constitutional legal regulations in compliance with the constitutional order, which in this case implies their duty to examine, in every specific matter, whether apart from identifying the telecommunication traffic data of a specific person there is not, in respect to the seriousness of the criminal offence, any other possibility to achieve the goal of the criminal proceedings otherwise or whether*

90 Decision of the Constitutional Court file number Pl. ÚS 24/11, 43/2012 Sb., N 217/63 SbNU 483, English translation available at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Decisions/pdf/Pl_US_24-11.pdf.

it does not amount to an inadequate interference with the individual's fundamental right. It also considers important that the protection of fundamental rights and freedoms is subject to, in every individual case, review of an independent and impartial court, since decision making on issuing the relevant order is granted by the contested provision to the presiding judge or the judge within the preliminary proceedings, whereas such orders must be issued in writing and accompanied with reasoning. Nevertheless, these are guarantees that allow protection to be provided against an inadequate interference with the right to informational self-determination with respect to the facts of a particular case, yet they cannot eliminate the deficiencies consisting in indefiniteness and too general a character of the contested legal regulation in such a way that they would replace, on their own and in general terms, the consideration of the legislature on the intensity of a certain public interest in restricting a fundamental right or freedom in the case of individual criminal offences and the manner (i.e. specific form) of such restriction, including the aforementioned subsequent guarantees when disposing of the relevant data, which represent a political decision adopted within the limits defined by the constitutional order, with their own detailed abstract consideration. If adopted by courts, this approach would also be inconsistent with Art. 4, para. 2 of the Charter, pursuant to which limitations of the fundamental rights and freedoms may be placed upon them only by law, since only the legislature is provided with the constitutional capacity, upon imposing a certain duty, to give preference, at its own discretion and while respecting the proportionality principle, of the public interest approved by the constitutional order to the fundamental right in a type-defined legal relation. Furthermore, leaving the determination of the constitutionally constituent limits only on the decision-making practice of courts would not be consistent with the requirement of legal certainty, since any potential interference with the right to informational self-determination is not, as a consequence of the indefiniteness of the current legal regulation, predictable for the individual to such an extent that would correspond to the seriousness of any possible negative effects onto their privacy. It may thus be stated that it is this indefiniteness that represents the primary deficiency of the contested legal regulation, as far as its constitutional review is concerned."

3.3 Differentiation and classification of powers in the law of criminal procedure

The coercive powers related to telecommunications data are relatively precisely defined in the criminal procedure. In that respect, Czech law is relatively specific by having a bi-lateral regulation of interception of electronic communications and retention of traffic metadata. That means that the duties and procedures that apply on the side of the providers of electronic communications services are defined in the Act on Electronic Communications, while the procedures that apply on the side of the Police or the public prosecution are laid down in the Code of Criminal Procedure. The reason for such dichotomy lies in the fact that wiretapping and data retention serve other purposes than just criminal procedure. Consequently, the provisions laid down in the Act on Electronic Communications cover in general the obligations of the providers of services of electronic communications and specify only the purposes for which the given data might be requested. The procedures of requesting these data as such are then laid down in specific Acts (incl. the Code of Criminal Procedure).

The relevant provision of the Act on Electronic Communications is section 97 and the relevant provisions of the Code of Criminal Procedure are sections 88 and 88a.

It is to be noted that, despite having a formal opportunity to request wiretapping or retained traffic data, *de facto*, the Police has extremely limited options to use this coercive power in criminal proceedings. As a result, in practice there are no situations in which the Police requests wiretapping or traffic data for the purposes of criminal procedure directly – when the given data is needed for use in a criminal procedure, such requests are always made through the Public Prosecution Office.

As noted earlier, there are, apart from traffic data, no specific procedural rules for the various coercive powers to obtain stored communications. Consequently, stored communications are gathered and forensically used based on the general rules, which enable the Police or the Public Prosecution to secure assets, request information, conduct surveillance etc.

4 INTERCEPTION OF CONTENT DATA

4.1 Object of interception

Like in most modern countries, the Czech law contains one key provision in the criminal procedure law, that deals with interception of the content of communication in transmission – Section 88 of the Criminal Procedure Code.

According to this provision, the object of interception is broadly specified as "telecommunications traffic". Neither legislature nor case law however deals with the definition of this term. Traditionally, this term means communication between persons via landlines, mobile phones, fax, radio or similar devices. However, due to technological development, the interpretation of has evolved. Nowadays it would probably cover all sorts of communication transferred via telecommunications and electronic communications networks, including communication between computers or other communication devices, as well as any kind of IP traffic, regardless of whether it was generated by persons or computers. Even content data transferred while one is surfing the web via electronic communications networks would probably be subject to interception.

When defining the term "telecommunications traffic", literature usually refers to the Act on Electronic Communications.[91] This act in itself does not contain a definition of the term, but we may understand it as content transferred via electronic communications networks, which are defined by the act as transmission systems and, where applicable, switching or routing equipment and other facilities, including network elements, which are inactive and which permit the conveyance of signals.[92]

Another suggestion may be found elsewhere in the Act on Electronic Communications, specifically in Section 89, which deals with the confidentiality of communication. Based on this provision and other clues, we may

91 For example Šámal, P. et al. *Trestní řád: komentář*. 7., extended release, Praha: C. H. Beck, 2013, xxii, 1898 p.

92 Section 2 letter h) of the Act No. 127/2005 Sb. on electronic communications.

conclude that telecommunications traffic may be defined as any data transferred via public electronic communications networks between a finite number of subscribers or users. Since it is impossible to tell in advance whether intercepted electronic communication will or will not contain such data, any interception should be done only after an interception order is issued.

The abovementioned provision of the Criminal Procedure Code therefore covers access to ongoing electronic communication. The Police may, once it has received the interception order, intercept any data that are "in traffic" – from the moment they are sent from the source device to the moment they are received by the destination device. Which means that it also covers the interception of electronic communication data, which are temporarily stored during the process of transmission.

There is also debate on whether the interception order also covers transmission outside of the network. Recently a decision has been issued, mentioning that an interception record also contained a conversation, which was taking place near a phone connected to another phone at the time of the interception[93]. According to technicians, the phone transmits surrounding sounds even before the other party of the call picks up the phone and judging from the decision mentioned above, even these sounds are part of interception record. The use of such a record as evidence is rather problematic, because nobody can reasonably expect the phone to transmit the surrounding sounds to the provider even before the call itself begins. However, there is at the moment no case law to clarify this matter.

Electronic communication data, which are stored before or after the process of transmission (e.g. email drafts or sent emails, emails stored by the provider, received emails stored by the recipient or completely web-based communication, for example on social networks), are not protected by the telecommunication secrecy, but are recognized as documents stored in private, which means that the access to such data is governed by different provisions of the Criminal Procedure Code.

Since the Criminal Procedure Code is rather outdated, it does not address access to data or stored electronic communication in detail. The only

93 Page 50 of the decision of the City court in Prague from 30. 4. 2014 No. 42 T 8/2013. Available in Czech at http://www.pecina.cz/files/Rozsudek_MS-P_30. 4. 2014.pdf.

detailed rules are related to access to the traffic and location data retained by electronic communications service providers[94]. Apart from that, there are no specific provisions providing clear rules for accessing stored communication data. Therefore, when there is need to access such data, law enforcement authorities are forced to apply more general rules, which were originally made for different purposes.

The methods usually used for accessing electronic communication data stored before the beginning or after the end of telecommunication transmission (message drafts, sent messages, stored received messages, etc.) vary depending on the source of such data.

The communication data may be stored on a device (hard drives, flash drives, mobile phones, computers, etc.), which may be acquired following the provisions on Obligation to release property[95], or Seizure of property[96], seized during house or personal searches[97] or examined[98]. Such communication data can be accessed without further consent from the judge or public prosecutor. There is also some discussion as to what data are considered to be stored in the seized computer system. For example, according to some interpretations, even communications data that are stored in a connected cloud storage, may be accessed from the seized device without further consent, because they are considered a part of such a computer system. There is, however, no official opinion or judicial decision to clarify this matter.

If the data is stored elsewhere (by the provider, in the cloud, on someone else's device etc.), then it is protected as records stored in private and may be accessed only with prior consent of the judge (surveillance of persons or items[99]), or prior consent of the respective user. This approach is also

94 Section 88a of the Act No. 141/1961 Sb. code of criminal procedure.
95 Section 78 of the Act No. 141/1961 Sb. code of criminal procedure.
96 Section 79 of the Act No. 141/1961 Sb. code of criminal procedure.
97 Section 82 of the Act No. 141/1961 Sb. code of criminal procedure.
98 Section 113 of the Act No. 141/1961 Sb. code of criminal procedure.
99 Section 158d of the Act No. 141/1961 Sb. code of criminal procedure.

supported by the Opinion No. 1/2015 of the Supreme Public Prosecutors Office, which states: [100]

> *"The current content of the email inbox is determined by the will of the user and can be accessed following the rules stipulated in section 158d para. 3. of the Code of Criminal Procedure, which can be considered a legal license to overcome the constitutional right to privacy of records located in an email inbox […]"*

However, this applies only to the data stored on the device or on the server at the moment of the seizure or first access. Should the seized device or obtained access be used for further interception of transmissions received in the future, an order for interception and recording of telecommunications is necessary. This is also supported by the opinion cited above, which in the para. 3 states:

> *"Access to the e-mail communication in real time is possible only following the rules specified in section 88 para. 1 of the Code of Criminal Procedure, because, like the telecommunications traffic, it also takes place in an electronic communications network."*

The Czech government is aware of the obsolescence of the Code of Criminal Procedure and is therefore preparing its complete recodification. As far as we know, during this process the possibility of introducing specific provisions for access to electronic data, including communication data, has also been discussed. However, the entire process of recodification is in its infancy and so we cannot expect any substantial changes in the legislation in the near future.

4.2 Special protection of confidential communication content

The provision on interception of electronic communication only provides protection for the communication between the defence counsel and the accused. Such communication is inadmissible in criminal proceedings and if the police authority finds during the interception that the accused has been communicating with their defence counsel, they are obliged

100 Opinion No. 1/2015 of the Supreme Public Prosecutors Office, on the harmonization of interpretation of laws dealing with access to mobile devices and other storage media, including the content of e-mail inboxes. This document is not available in English, translation by the author.

to immediately destroy the interception record and not to use the information obtained in this context in any way[101]. These rules are deemed rather problematic by some sources. The reason is that most interceptions are conducted before the commencement of the criminal prosecution and in this stage, the person against whom the criminal proceedings are conducted is not related to as the accused. Therefore, a *stricto sensu* interpretation of the provision would mean that before the commencement of the criminal prosecution, the police would be able access and use even the communication between the persons against whom the criminal proceedings are conducted and their attorney. Some sources see this as an intrusion into the right to a fair trial[102].

Also, the protection of communication between the defence counsel and the accused is not absolute. Particularly when the communication relates to a crime, which has been committed by the defence counsel in cooperation with the accused, the protection does not apply. This approach is supported in the decision of the Constitutional Court No. I.ÚS 1638/14, which states (informal translation): [103]

> *"However, as is clear from the case law of the European Court of Human Rights and of the Supreme Court, the protection of communication between a solicitor and their client is not absolute, inviolable and may be limited in certain circumstances. Any possible criminal activity of the solicitor, both to the detriment of the client or to the detriment of others in complicity with the client, cannot be considered provision of legal services, and in such case it is impossible to provide any protection of such activity."*

4.3 Execution of telecommunication interception

According to the Act No. 237/2008 Sb. on Police of the Czech Republic, these activities are conducted by the Czech Police as is laid down in Section 19.

101 Section 88 paragraph 1 of the Act No. 141/1961 Sb. code of criminal procedure.

102 For example in Czech see Vantuch, P. Nová úprava odposlechu v trestním řádu od 1. 7. 2008. *Bulletin advokacie*, 2008, No. 10, p. 29.

103 Decision of the Constitutional Court file number I. ÚS 1638/14. Available online in Czech at http://nalus.usoud.cz/Search/GetText.aspx?sz=1-1638-14_1. Provided excerpt translated by the author.

A special unit of the Police called the Unit for Special Activities is responsible for conducting the interception itself. The Unit for Special Activities is a specialized unit, which carries out interception and recording of telecommunications traffic and surveillance of persons and items for authorized security and law enforcement bodies, in accordance with the Code of Criminal Procedure, the Act on Police of the Czech Republic and other relevant legislation. It is the only unit authorized to conduct these operations and this position is reflected in its organizational structure – its headquarters is located in Prague and it also has subsidiaries in each region of the Czech Republic. Every interception order is forwarded to this unit, which subsequently carries it out. The recordings of intercepted traffic are then provided to the investigator who is responsible for the respective criminal investigation.

The criminal law does not stipulate which modes law enforcement authorities should use when executing the interception. The specific methods they use are also kept confidential, but as far as the we know, the Police usually intercept the communication itself using dedicated access points, which the ISPs are obliged to install into their infrastructures.[104] They can probably also intercept the communication without any recourse to third parties (ISPs) by using special equipment and tools, even though it is not very usual. When it is practical, the police may also order the ISP to extract and surrender specific stored communication data.

There are no accompanying investigative measures mentioned in the main provision itself. Law enforcement authorities may, however, follow different provisions in order to access houses or other places[105] or to be able to use specific technical measures to gain access to the communication.[106]

4.4 Duties of telecommunication service providers to cooperate

The duty of ISPs to cooperate in the interception is stipulated in the Act No. 127/2005 Sb. on electronic communications (Act on Electronic

104 See Section 97 of the Act No. 127/2005 Sb. on electronic communications.
105 See Section 82 of the Act No. 141/1961 Sb. on Criminal Procedure.
106 See Section 158d of the Act No. 141/1961 Sb. on Criminal Procedure Code.

Communications), which obliges entities providing public communication networks or publicly available electronic communications services to install specific equipment for interception into their infrastructures and to cooperate during the interception (see below). These entities are defined in Section 2 of the Act.

It is important to note that these obligations apply only to providers of network infrastructures or electronic communications services, which are licensed by the Czech Telecommunications Office. Therefore, providers of services of information society[107] (IP-application level – Internet applications, cloud, email services, social networks, etc.), for example, are not specifically obliged to provide such cooperation.

More specifically, according to Section 97 of the Act on Electronic Communications, an entity providing a public communications network (infrastructure providers working on the IP-transport level) or a publicly available electronic communications service (access providers on the IP-transport level) is required to allow interception and recording of transferred communication at the expense of the police.

According to this provision, these providers are required to install a dedicated interface into their infrastructures, which the Unit for Special Activities can use to connect their devices used for accessing ongoing traffic.

This duty is described in detail in the decree No. 336/2005 Sb. In accordance with this decree, providers and the police shall agree on the technical parameters of the equipment, which the provider will purchase and install into the network or service to provide an interface for connecting devices for wiretapping:[108]

> *"Section 7*
>
> *(1) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service (hereinafter referred to as "operator") shall equip their network or service with interface for connecting devices for interception on the basis of a request from a competent authority.*

107 According to the Act No. 480/2004 Sb. on some services of the information society.

108 Decree No. 336/2005 Sb. on technical and operational conditions and points of connection of the telecommunications equipment for interception and recording of telecommunications traffic. This decree isn't available in English to date. The cited provision was translated by the author.

(2) If the operator is developing a new network or service, significantly expanding or changing the existing network or service, they shall prompt the competent authority to issue a request for equipping the network or service with an interface for connecting interception devices. The competent authority shall issue the request within 15 days from the prompting.

(3) On the basis of request issued according to the paragraph 1 or 2, the operator in cooperation with the competent authority shall propose possible technical solutions, including the reasons for their implementation and a calculation of the cost of each solution.

(4) The chosen solution and its parameters shall be specified in a record jointly elaborated by the competent authority and the operator. The record shall also include a calculation of financial costs and the method and schedule of the payment."

The methods of transfer of intercepted data from the ISPs to the Police are described in Section 13 of the decree No. 336/2005 Sb., according to which the intercepted communication is transferred to the police via a hard data link or a secure virtual channel on the Internet (using the standardized communication protocol SFTP – the provider accesses the police server). The provided data should be equipped with a specific identifier and a timestamp. The integrity of the data is to be ensured by creating a fingerprint using the SHA-1 hash function. The intercepted emails may be sent to the Police also via a dedicated SMTP server. The respective provision states:[109]

"Packet networks outputs

Section 13

(1) The output of the network or service is provided via a) a hard data link, or b) a secure virtual channel on the Internet using the standardized communication protocol FTP, server shall be provided by a competent authority and operator should connect as a client.

(2) The sent data unit shall be equipped with an identifier of user address and a serial number or a time stamp. The data integrity of the data unit shall be ensured by creating a file stamp using the hash function SHA-1.

[109] Section 13 of the decree No. 336/2005 Sb. on technical and operational conditions and points of connection of the telecommunications equipment for interception and recording of telecommunications traffic. This decree isn't available in English to date. The cited provision was translated by the author.

> *(3) During the interception of emails, the operator may, with consent from the competent authority, send copies of messages using protocol for transferring email to the SMTP server provided by the competent authority."*

As far as we know, there are no checks and filtering obligations for providers mentioned in the statutory law. ISPs (providers of a public communication network or a publicly available electronic communications service) are, however, according to Section 97 paragraph 6 of the Act on Electronic Communications, obliged to provide access to decrypted traffic if they are using any form of encryption.

If the communication is encrypted by the user, or by the provider of IP-application level services, then the ISP is not obliged to assist competent authorities in decrypting it in any way. Also, these rules do not apply to providers of information society services (IP-application level), although they may be required to provide access to decrypted communications data by the police authority if it is necessary for the success of surveillance of persons and items, according to section 158d para. 9 of the Code of Criminal Procedure.

4.5 Formal prerequisites of interception orders

The interception of electronic communications may be conducted only after there is a valid interception order, which is a decision *sui generis*.

Only the public prosecutor may apply for the interception order in preliminary proceedings, usually after consultation with the police investigator. Before submitting the application, the public prosecutor usually verifies whether the criminal proceedings are being conducted for a crime, for which the interception can be ordered. He particularly assesses whether the offence described in the record of the commencement of the criminal proceeding or in the resolution to initiate the criminal prosecution corresponds with the used legal classification. He also assesses whether it may be reasonably assumed that the interception will yield facts relevant to the criminal proceedings and whether there is no other way to achieve such purpose or whether its achievement would be otherwise significantly reduced.

The justified application is then presented to the judge, who can authorize the interception by issuing the order, according to the section 88 para. 2 of the Code of Criminal Procedure:

> *"Interception and Recording of Telecommunications*
>
> *Section 88*
>
> *(2) The presiding judge and, in preliminary proceedings upon the petition of the public prosecutor, the judge, is entitled to warrant the interception and recording of telecommunications. […] The order for the interception and recording of telecommunications shall immediately be forwarded to the police authority. In the preliminary hearing, the judge shall send a copy of the order for the interception and recording of telecommunications to the public prosecutor without undue delay."*

This procedure is described in detail in the section 32 of the instruction of the Ministry of Justice Ref. No. 505/2001-Org, which issues the internal and office directive for courts: [110]

> *"Section 32*
>
> *Interception and Recording of telecommunications*
>
> *(1) The judge shall, at the time of availability, apply the procedure described in section 27 para. 1.*
>
> *(2) The judge shall decide on the application of the public prosecutor for interception and recording of telecommunications traffic in accordance with section 88 para. 2 of the Code of Criminal Procedure (hereinafter referred to as "interception") without delay or within the period agreed with the public prosecutor; on the proposal of the public prosecutor to extend the duration of the interception (section 88 para. 4 of the Code of Criminal Procedure), the judge will decide no later than on the last working day before the expiry of the previously issued interception order, if the public prosecutor filed the proposal at least 3 working days before the expiry of the interception order."*

The order is then forwarded to the investigator and to the Unit for Special Activities, which carries out the interception.

110 Instruction of the Ministry of Justice Ref. No. 505/2001-Org, which issues the internal and office directive for courts. Provided provision translated by the author.

The application for interception order, according to the Art. 67 of the binding guideline of the Police President No. 30/2009 Sb. on the tasks in criminal proceedings,[111] usually contains the following information:

a) the identifier of the device or the user, if his identity is known,
b) the specific facts about the case, which justify the need to issue the interception order, and its duration,
c) if the criminal proceedings are conducted for an intentional criminal offence, for which prosecution is stipulated in a declared international treaty, a reference to this international treaty,
d) a description of the offence and its legal classification,
e) a list of interception orders already issued for the same identifier,
f) the application for an interception order itself.

The complexity of the justification and description of the case in individual applications varies depending on the complexity of each case. The application may also be submitted with investigative files or other additional materials.

Applications are submitted to the court in written form. The basic formal requirements for the interception orders themselves are defined in the section 88 para. 2 of the Code of Criminal Procedure as follows:

> "*[…] The order for interception and recording of the telecommunications service shall include a determined user address or a user device and the user if their identity is known, and the period during which the interception and recording of telecommunications traffic is conducted cannot be longer than four months; the justification of the order must include the specific facts that justify the issue of such order as well as its period. […]*"

The Constitutional Court has also dealt with the formal requirements of interception orders in its Decision number II. ÚS 615/06.[112] According to it, an interception order must be supported by relevant clues from which one can derive a reasonable suspicion of committing a crime. The mere existence of a criminal complaint is not a sufficient justification for issuing the interception order. In addition, the court stated that the interception

111 Binding guideline of the Police President No. 30/2009 Sb. on the tasks in criminal proceedings. In Czech available online at http://www.pecina.cz/files/pokyn2.pdf.

112 Decision of the Constitutional Court file number II. ÚS 615/06-1, N 88/45 SbNU 291.

order must be individualized in relation to a specific person or device. The order must also specifically state what facts relevant to the criminal proceedings would probably be obtained. The court also criticized the practice of some interception orders being issued, even though the material conditions of the case had not been sufficiently assessed. The interception order also must therefore contain an assessment of these conditions.

Based on these findings, the interception order should contain at least:

a) the order of interception,
b) an identifier of the user or the device,
c) the name of the user, if it is known (name, address, etc.),
d) an identification of the crime, for which the criminal proceedings is conducted (a reference to an international treaty if applicable),
e) the duration of the interception (no longer than 4 months).

Additionally, the justification of the order should include:

a) specific facts about the case, which justify the issuance of the interception order and its duration,
b) the purpose of the interception,
c) an explanation of the reason why there is no other way to achieve the purpose or why its achievement would otherwise be significantly reduced.

4.6 Substantive prerequisites of interception orders

According to Section 88 para. 1 of the Criminal Procedure Code, the interception order can be justified by the following crimes:

- machinations in insolvency proceedings,
- violation of regulations on the rules of competition,
- negotiating advantages during public procurement, tender and auction,
- machinations during public procurement and tenders,
- machinations at a public auction,
- misuse of the powers of an official person, or other intentional criminal offence for which prosecution is stipulated in a declared international treaty.

Additionally, it may be justified also by crimes for which the law stipulates a prison sentence with the upper penalty limit of at least eight years.

Any user and any device that fall within the scope of the Act on Electronic Communications may be subject to an interception order if the required criteria are met and if the judge considers the reasoning of the application sufficient. Since the interception order must include a determined user address or user device, it cannot target any particular communication content, but only a particular person or device. A user is, according to section 2 of the Act on Electronic Communications, defined as "anyone who uses or requests a publicly available electronic communications service", so it includes users of IP-transport level services as well as users of IP-application level services.

The order for the interception and recording of telecommunications may be issued if it may be reasonably assumed that facts relevant to the criminal proceedings will be obtained this way and if there is no other way to achieve such purpose or if its achievement would be otherwise significantly reduced[113]. The investigator, the public prosecutor and most importantly the judge should therefore consider whether the specific facts relevant for criminal proceedings cannot be secured by other, less intrusive means of investigation referred to in the Code of Criminal Procedure.

This approach is based upon basic principles of criminal proceedings defined in the section 2 of the Code of Criminal Procedure, especially on the principle of proportionality and the principle of moderation formulated in Section 2 para. 4 as follows:

> "*[…]Criminal cases shall be dealt with a full investigation of rights and freedoms guaranteed by the Charter of Fundamental Rights and Freedoms and by international treaties on human rights and fundamental freedoms that the Czech Republic is bound by; when conducting acts of criminal proceedings, the rights of persons that such acts affect may be intervened only when justified by law and to the extent necessary to ensure the purpose of criminal proceedings.[…]*"

There is no additional obligation for the authorizing authority to verify that the interception is proportionate to the seriousness of the offence in the individual case. The proportionality is, however, always assessed in the interception order. For example, if in one case the police authority

113 Section 88 paragraph 1 of the Act No. 141/1961 Sb. Code of Criminal Procedure.

applied for too many interception orders, the judge would probably refuse to issue it, because he would find it disproportionate and against principle of moderation formulated in the section 2 para. 4 of the Code of Criminal Procedure cited above.

The required degree of suspicion is not specified in the positive law, but it usually is evaluated on a case by case basis by the judge. In some interception orders judges did not assess the degree of suspicion enough, which is why the Constitutional Court stated in the supra cited decision that the order should contain at least relevant clues, from which one can derive reasonable suspicion of committing the specified crime.

The maximum length of an interception order is 4 months, and based on the assessment of the current course of the interception, the judge of a superior court and, in the preliminary hearing upon a petition of the public prosecutor, a deputy county court judge may extend the duration of the interception and recording of telecommunications traffic even repeatedly; however, always only for a maximum period of four months.

There is no positive provision that deals with the possibility of revocation of the interception order. However, in our opinion, the issuing judge may decide to revoke the order when a lack of substantive prerequisites for the interception becomes apparent. Also the Constitutional court may revoke the interception order.

According to Section 88 para. 8 of the Code of Criminal Procedure, the Supreme Court may subsequently review the legality of the interception order, following the procedure described in sections 314l – 314 n of the Code of Criminal Procedure.

The police authority is also obliged to continuously assess whether the reasons, which led to the order for the interception and recording of telecommunications 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 period, for which the interception order was issued. They also must immediately notify in writing the judge who issued the order for the interception and recording of telecommunications.[114]

114 Section 88 paragraph 3 of the Act No. 141/1961 Sb. Code of Criminal Procedure.

4.7 Consent by a communication participant to the measure

The law enforcement authority may also order the provider to intercept and record telecommunications or conduct it themselves, even without the interception order, but only if the user of the intercepted unit agrees to such a measure and if the interception is conducted in connection with a criminal proceeding for following criminal offences:

- human trafficking,
- the delegation of the custody of a child to someone else,
- restriction of personal freedoms,
- extortion,
- kidnapping of a child or persons suffering from a mental disorder,
- violence against a group of people or an individual,
- dangerous threats, or dangerous persecution[115].

This provision is in some sources criticized because it infringes the telecommunications secrecy of the other intercepted user, who did not provide the consent. Normally, such infringement is justified on the basis of a proper court order, in which the judge assesses whether there is a reasonable justification for interception. However, in this case the protection is somewhat weaker. On the other hand, some kind of protection is provided according to the General Instruction of the Supreme Public Prosecutor No. 8/2009, on criminal proceedings, which states in Section 45: [116]

> *"Section 45*
>
> *Interception without court order*
>
> *The public prosecutor shall make sure, that if a police authority orders the interception and recording of telecommunication without a court order, it shall inform him immediately. The public prosecutor then assesses whether the interception was ordered in the criminal proceedings for the offence, for which it is possible to use this measure, and that throughout the period of interception such qualification is justified. If the public prosecutor determines that the interception could not lead to obtaining facts important for the criminal proceedings, or that the consent is invalid or was waived, he orders the police authority to immediately discontinue*

115 Section 88 paragraph 5 of the Act No. 141/1961 Sb. Code of Criminal Procedure.

116 General Instruction of the Supreme Public Prosecutor No. 8/2009, on criminal proceedings.

the interception and destroy the obtained records. The obtained information cannot be used further in this case. If the interception is ordered by the public prosecutor, the provisions on the interception ordered by the judge shall apply adequately."

4.8 Duties to record, report, and destroy

The intercepted data and communications are stored by the Unit for Special Activities in a secure storage, and provided to the police investigator. He then assesses the content of the data and prepares an interception record – a document, which usually contains a transcript of the parts of the communication, which are relevant to the criminal proceedings. If the record is to be used as evidence in the criminal proceedings, it needs to be accompanied with a protocol. The protocol must, according to Section 88 para. 6 of the Code of Criminal Procedure, contain information about the place where the interception was conducted, the time of the interception, the manner of the interception, the authority that issued the record, and general information about the contents of the record. The protocol must also contain the general information required by Section 55 of the Code of Criminal procedure.

The police authority is not obliged to provide any reports on the progress of the interception or any other final report to the judge. The record is, however, available to the public prosecutor, who should regularly assess its content and the legality of the interception.

If the interception did not help to find any facts relevant to the criminal proceedings, the police authority, after approval from the court or the public prosecutor in preliminary hearings, must immediately destroy all records after three years from the final conclusion of the matter.[117]

If the police authority was informed about an extraordinary appeal within the set deadline, they shall destroy the records of the interception after the decision on the extraordinary appeal or after a final conclusion on the matter.

The police authority is responsible for the destruction of the record and it also must send a transcript on the destruction of the record of the interception

117 Section 88 paragraph 7 of the Act No. 141/1961 Sb. code of criminal procedure.

to the public prosecutor, whose decision finally concluded the matter or, in the proceedings before a court hearing, to the presiding judge in the first instance, for the record on file. The police authority must also order the Unit for Special Activities to destroy their respective records.

Also, if the police authority finds during the interception and recording of telecommunications that the accused has communicated with their defence counsel, they are obliged to immediately destroy the relevant part of the interception recording. In this case the report on the destruction of the record should be placed in the file.[118]

4.9 Notification duties and remedies

After the final conclusion of the matter the public prosecutor or the police authority, by whose decision the case was finally concluded, or the presiding judge in the first instance in the proceedings before a court hearing shall inform the affected person, if their identity is known, about the interception and recording of telecommunications service.[119] The information should include the designation of the court that issued an order for the interception, the duration of the interception and the date of the conclusion.

The information about the interception is not provided to the affected person in cases when:

- the criminal proceedings is conducted for specific crimes,
- the criminal offence involved more people and in relation to at least one of them the criminal proceedings have not yet been finally concluded,
- it could lead to threats to national security, life, health, or the rights and freedoms of individuals, etc.[120]

The affected person may file a petition to review the legality of the order for interception to the Supreme Court[121]. The procedure of the judicial review is described in the provisions 314l – 314n of the Code of Criminal Procedure.

118 Section 88 paragraph 1 of the Act No. 141/1961 Sb. code of criminal procedure.
119 Section 88 paragraph 8 of the Act No. 141/1961 Sb. code of criminal procedure.
120 See Section 88 paragraph 9 of the Act No. 141/1961 Sb. Code of Criminal Procedure.
121 Section 88 paragraph 8 of the Act No. 141/1961 Sb. Code of Criminal Procedure.

If the interception was conducted illegally, the officials conducting such interceptions may also be held liable for the criminal offence of violating the confidentiality of messages according to Section 182 of the Code of Criminal Procedure. They and also the judge who issued the illegal interception order may be held liable for the criminal offence of abuse of powers of an official person according to Section 329 of Code of Criminal Procedure.

The legality of interception is also controlled by a Parliamentary Commission for monitoring the use of interception and recording of telecommunications traffic, according to Section 98 of the Act on Police of the Czech Republic.

4.10 Confidentiality requirements

The information about specific measures implemented to allow communication interception is classified (reserved) according to the act No. 412/2005 Sb. on the protection of classified information.[122] If anyone discloses classified information to an unauthorised person, they may be, according to Section 140 of the Act on the Protection of Classified Information, fined for an administrative offence with a fine of up to 5,000,000 Czech crowns and also prosecuted for the criminal offence of endangering classified information according to Section 317 or 318 of the Criminal Code.

ISPs and their employees are also required to maintain confidentiality of any tapping or recording of traffic and data, according to Section 97 para. 8 of the Act on Electronic Communications. The ISP may be fined according to the section 118 of the Act on Electronic Communications for violating this duty of confidentiality in the amount up to 20.000.000 Czech crowns.

122 Act No. 412/2005 Sb. on the protection of classified information. This act is not available in English.

5 COLLECTION AND USE OF TRAFFIC AND SUBSCRIBER DATA

5.1 Collection of traffic data

The most important provision relevant to the collection of traffic and subscriber data is Section 88a of the Code of Criminal Procedure.

Additionally, traffic data not protected by the telecommunications secrecy or by the protection of personal and intermediation data may be requested following the procedure stipulated in Section 66 paragraph 3 of the Act No. 273/2008 Sb. on the Police of the Czech Republic.

Section 88a of the Code of Criminal Procedure specifies the types of crime for which the retained traffic data may be requested. The general requirement is that the prosecuted crime should be an intentional one, for which the law allows for imprisonment with an upper limit of the penalty of at least three years. This, however, does not apply for the exhaustive list of crimes, which cannot be practically prosecuted without traffic and location data, i.e. crimes committed by means of electronic communication.[123] As the Explanatory Memorandum states "*should the police during investigation of these crimes have no chance to get traffic and location data, one could consider the decriminalization of such conduct, as these crimes would be virtually inexplicable.*"[124] Finally, the data could be also requested for the purposes of criminal proceedings for an intentional crime, which the Czech Republic has to prosecute pursuant to an international treaty, which is binding the Czech Republic.

---

123 The full list with the relevant section of the Penal Code No. 40/2009 Sb. includes the following crimes: violating the secrecy of conveyed messages (Sec. 182), fraud (Sec. 209) unlawfully gained access to computer system or data carrier (Sec. 230) acquisition and receipt of access equipment or codes for computer systems or other similar data (Sec. 231), criminal threat (Sec. 353), stalking (Sec. 354), spreading of false news (Sec. 357), incitement (Sec. 364) and criminal connivance (Sec. 365).

124 Explanatory Memorandum to the Act No. 127/2005 Sb. On electronic communications and on amendment to some related laws (Electronic Communications Act), as amended, and certain other laws. Available online in Czech: http://www.psp.cz/sqw/text/orig2.sqw?idd=84557.

The provision cited supra also states that the order for the ascertainment of data on the telecommunications service can be issued only when there is no other way to achieve the pursued purpose or when its achievement would otherwise be significantly harder.

The application for a court order to request traffic data is prepared in the preliminary proceedings by the public prosecutor, usually on the basis of a written and reasoned proposal from the police authority. Before he submits the application, he must assess whether the order is necessary in order to obtain facts relevant to criminal proceedings, whether there is no other way to achieve the pursued purpose, whether the criminal proceedings are conducted for an adequate criminal offence and whether he has enough information about the case to properly determine what data are to be obtained. He should mention these facts in the application in which he also indicates the scope of the required data and formulates a proper justification.[125] The completed application is then forwarded to the judge, who evaluates the provided information and, if satisfied, issues the order to request traffic data. The order usually contains more or less the same information as the application. The order is then forwarded to the public prosecutor.

The duty of ISPs to retain and subsequently disclose traffic data is specifically mentioned in Section 97 paragraph 3 of the Act on Electronic Communications.

According to this provision, ISPs (of services on IP-transport level) are required to retain specific traffic data for a period of 6 months. General categories of data that are subject to data retention are mentioned in para. 4 of the respective provision; a more detailed list of these data is specified in Section 3 of the decree No. 357/2012 Sb. on storing, handing over and liquidation of traffic and location data, which is not available in English. The data to be retained may be divided into two general groups:

- data used for identification of the source and the recipient of the data communication (telephone numbers, IMEIs, IP addresses, MAC addresses, port number, IMSI identifier, account identifier – email, username etc.)

125 According to the General Instruction of the Supreme Public Prosecutor No. 8/2009, on criminal proceedings.

- data used for identification of the date, time, manner and duration of the communication (communications protocol details, type of communication, time and date of the communication, duration, length, etc.).

Providers of information society services (IP-application level) are not specifically required to retain any traffic data; however, they do so with the consent of users. The extent of the data that are retained in this manner varies depending on the type of service.[126]

In practice orders to request traffic data are usually carefully evaluated by the ISPs themselves. If the order is not specific enough or does not contain all the information required by the law, they usually refuse to release the data.

As of now it is not possible to access traffic data by an automated online procedure. The only authority that can request traffic data from ISPs is the Unit for Special Activities. They usually send the request to an ISP via email to the ISP, who, upon such request, releases the requested data in the prescribed format. The Unit for Special Activities then forwards the data to the police authority.

5.2 Collection of subscriber data

Subscriber data could be requested from providers of a public communications network or a publicly available electronic communications service (IP-transport level services) following the same procedure as in the case of traffic data – Section 88a of the Code of Criminal Procedure.

A different procedure applies if the subscriber data is requested from ISPs providing services on an IP-application level according to the Act on Information Society Services. In this case the subscriber data may be requested from the provider of IP-application level services using a production order issued by the police or a public prosecutor according to Section 8 of the Code of Criminal Procedure. If the respective subscriber data are subject to an obligation of secrecy, then they may be requested for

126 For example social media services usually retain a lots of traffic and location data whereas hosting providers retain just a few.

criminal proceedings upon prior consent of the judge (Section 8 para. 5). This of course does not affect the obligation of confidentiality of an attorney under the Advocacy Act.

The communication data may be requested from ISPs of IP-transport level services in cases specifically stipulated[127] in Section 88a of the Code of Criminal Procedure upon order issued by the judge based on an application by the public prosecutor. The formal requirements are the same as in the case of the order to release traffic data. The subscriber data may be also requested directly by the police according to Section 66.

5.3 "Data retention"

The "full-scale" data retention framework was first introduced in 2005 by the Act on Electronic Communications. The act contained quite a vague formulation that was in substantive parts linked to the implementing Decree No. 485/2005 Sb., on the extent of traffic and location data, the period of time for which such data are retained and the manner in which they are submitted to bodies authorised to use the data, which laid down the technical details. This whole data retention regulation was rather unclear and loose.

After the adoption of the Data Retention Directive[128] in 2006 the Act was amended by the Act No. 247/2008 Sb. However, with regard to the extent of the data to be retained, the Czech implementation went far beyond what was requested by the Directive. Namely the amount of transferred data, IMEI and SIM cards relations and the type of encryption of the communication had to be retained.

After harsh criticism of the data retention framework in the Czech Republic, a group of MPs and Senators submitted a petition to the Constitutional Court requesting a review of the constitutionality of the framework and

127 If the criminal procedure is conducted for the listed crimes and if there is no other way to achieve the pursued purpose or if its achievement would be otherwise significantly harder.

128 Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

an annulment of the relevant provisions. The Constitutional Court ruled on it in the Decision file number Pl. ÚS 24/10,[129] which was described in the second chapter.

The new version of data retention was introduced in 2012 by the Act No. 273/2012 Sb. amending Act on Electronic Communications, and certain other laws. The technical details were prescribed by Decree No. 357/2012 on storing, handing over and liquidation of traffic and location data. The new wording of Section 97 entails an exhaustive enumeration of the subjects that may request the data. A new section 88a of the Act on Electronic Communications was also added, requiring ISPs to ensure the security and confidentiality of the retained data, and ordering them to destroy them in an irreversible manner. According to the new wording of Section 97 of the Act on Electronic Communications, ISPs are required to retain specific traffic data for the period of six months.

The following categories of data are subject to data retention:

- data used for identification of the source and recipient of the data communication (telephone numbers, IMEIs, IP addresses, MAC addresses, port number, IMSI identifier, account identifier – email, username etc.)
- data used for identification of the date, time, manner and duration of a communication (communications protocol details, type of communication, time and date of the communication, duration, length, etc.)

[129] Decision of the Constitutional Court file number Pl. ÚS 24/10, 94/2011 Sb., N 52/60 SbNU 625. English translation available at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=c574142df486769e0b435954fead08c3.

6 ACCESS TO (TEMPORARILY) STORED COMMUNICATION DATA

There is no specific provision that allows law enforcement authorities to access stored communications data, which is why they follow the procedures defined in more general provisions. In the past the fact that regional police units work rather independently led to situations, when different investigators and public prosecutors followed different general provisions for accessing stored data. For example, in South Moravian Region the law enforcement authorities accessed remotely stored email with order to request traffic data according to Section 88a of the Code of Criminal Procedure, whereas in the Pilsen Region the same data were accessed following provision 158d para. 3 of the Code of Criminal Procedure on surveillance of persons and items.

Since this situation led to many problems, the Supreme Public Prosecutors Office decided to harmonize the procedures applied by law enforcement authorities in different regions of the Czech Republic. Opinion No. 1/2015 of the Supreme Public Prosecutors Office, on the harmonization of interpretation of laws dealing with access to mobile devices and other storage media, including the content of e-mail inboxes states that for accessing stored communications data the procedure mentioned in Section 158d of the Criminal Procedure Code, the Surveillance of Persons and Items shall be followed.

A further description of the differences between the access to data in traffic and stored data is provided supra in chapter 4.1.

6.1 Online searches with the help of remote forensic software

Online searches are not regulated by any specific provision. There is also not a great deal of experience with using specialized remote forensic tools. However, it is probable that the police use them even for online searches, as an investigative measure. Various forensic tools could be probably used for online searches during the general surveillance of persons and items

according to Section 158d of the Code of Criminal Procedure. If the use of these technologies interferes with in the inviolability of residence, the confidentiality of correspondence, or the protection of the contents of other documents and records kept in private, then it may be performed only with a prior authorisation of a judge. However, because there is a lack of relevant case law, it is impossible to predict whether the use of such measures would be considered proportionate. In the opinion of the author of this chapter, the use of these measures would interfere at least with the principle of proportionality and the principle of moderation formulated in Section 2 para. 4 of the Code of Criminal Procedure. It can also be said that the evidence obtained this way would be probably considered inadmissible. The reason is that the rules on the surveillance of persons and items does not provide enough safeguards. Therefore, an introduction of a specific provision will probably be necessary in the future.

There are also known cases when such a measure was conducted by the victim in a state of self-defence or extreme emergency according to sections 28 and 29 of the Criminal Code.

The evidence gathered during the use of these measures must then be provided to the police authority for the purpose of criminal proceedings. There is some discussion in the Czech Republic about whether this is legal and proportionate and whether such evidence would be admissible.

6.2 Search and seizure of stored communication data

Due to the reasons mentioned supra, there are no special provisions dealing with the seizure of stored communication data in the Czech criminal procedure law.

As far as we know, the data itself cannot be seized; however, a police authority could seize a device or a storage medium, in which the data is stored (hard drives, flash drives, mobile phones, computers, etc.), following the provisions on the seizure of property (Section 79 of the Code of Criminal Procedure), or during house or personal searches (Section 82 of the Code of Criminal Procedure). Such data can be accessed and used without further consent from the judge or public prosecutor. According to Section 158d

of the Code of Criminal Procedure, law enforcement authorities can also access stored communication in a clandestine way during the surveillance of persons and items.

The safeguards and requirements for the interception of communication differ from those for access to stored data.

According to Section 88 of the Code of Criminal Procedure, the interception of communication may be conducted only if the respective criminal proceedings are conducted for specific crimes, if it may be reasonably assumed that facts relevant to the criminal proceedings will be obtained and if there is no other way to achieve such purpose or if its achievement would be otherwise significantly reduced, whereas in the case of access to stored data during the surveillance of persons and items (section 158d of the Code of Criminal Procedure) there are no such conditions.

Additionally, if the police authority wants to conduct interception, it always needs an order issued by the judge; in case of access to the stored data, the consent of the judge is necessary only if is going to interfere with in the inviolability of residence, the confidentiality of correspondence, or finding the contents of other documents and records kept in private with the use of technology.

Therefore, the legal protection of data in traffic is far better than the protection of stored data.

It is also not necessary to inform the suspect and/or the provider about the fact, that the law enforcement authorities accessed the stored communications data. But since the assistance from the provider is usually necessary, they have to inform at least him.

6.3 Duties to cooperate: production and decryption orders

In the Czech Republic, there is no special regulation providing cooperation duties for decoding encrypted data or handing over the necessary passwords.

However, everyone is required to comply with letters of request from law enforcement authorities for the performance of their actions without

an undue delay.[130] Such requests may even order anybody to decrypt data or to provide passwords. If the decrypted data or passwords are subject to an obligation of secrecy, they may be requested for criminal proceedings upon the prior consent of the judge.

The requested parties may, however, argue, that the disclosure of the requested information would interfere with their rights related to the principle of prohibition on self-incrimination, in which case they are not obliged to comply.

Since there is no specific provision and a lack of specific case law on this matter, it is difficult to guess what would happen if the police authority requested of the decrypted data or passwords. The author even tried to ask police investigators and public prosecutors whether they had any experience with such cases, but without any luck.

130 Section 8 paragraph 1 of the Act No. 141/1961 Sb. code of criminal procedure.

7 USE OF ELECTRONIC COMMUNICATION DATA IN JUDICIAL PROCEEDINGS

7.1 Use of electronic communication data in the law of criminal procedure

The Code of Criminal Procedure does not specifically regulate the situation of intercepted electronic communications data in criminal proceedings; thus it is necessary to follow general rules on the interception and recording of telecommunications under Section 88 of the Code of Criminal Procedure. This section does not make any difference between various forms of intercepted communication.

The basic requirement to order the recording of telecommunications for criminal proceedings is the drawing up of a protocol for such an order which must fulfill statutory requirements under Section 88 para. 6 of the Code of Criminal Procedure; it has to fulfill certain formal conditions. Lack of fulfillment of these conditions (particularly regarding information about the place, time, method of recording, the authority that issued the recording) can be overcome, even at the stage of criminal proceedings, in the same manner as any other formal defects in the protocol, e.g., hearing the person who participated in the performance of the act as the witness. This is not considered an inadmissible manipulation in the recording of telecommunication.

The content of the recording is also an essential requirement of the protocol related to the recording of telecommunication. The transcript of each part of the communication in such recording is, however, not an essential requirement of the protocol; it is sufficient to provide information about each part of the communication concerning the time, telephone numbers (or other identification related to other types of exchange of information), and identification of the participants in the exchange of information.[131]

131 Above stated was also confirmed in the decision of the High Court in Prague from 18 January 2001, file number 4 To 3/01.

Another important aspect when introducing the recording as evidence in criminal proceedings is its unaltered form. Assuming that, in the specific case, there is no apparent devaluation or any other reduction in the information value of the evidence, the applicability of the evidence in the criminal proceedings is not affected in any way. Technical measures to compress the content of intercepted communication cannot therefore be considered as unauthorized interference with the evidence in accordance with Section 88 of the Code of Criminal Procedure (such as the compression of communication on a data carrier). The use of only a part of the communication related to the criminal case is also considered admissible.[132]

The evidence itself could be presented in the form of the recordings (the recording is played at the stage of criminal proceedings where the evidence is presented) or in the form of the transcribed document containing the information from the recordings. It is however usual and recommended to present the intercepted material in transcribed form at the court.

The Code of Criminal Procedure does not specify in which form the collection of traffic and location data by providers of electronic communication under Section 88a should be presented at the criminal proceedings. There is no rigorous institute in the Code of Criminal Procedure to specify that. Such information is, however, presented as evidence and clarified in the criminal proceedings by an expert under Section 105 – 111 of the Code of Criminal Procedure. The data retained under Section 88a are used for identification of the source and the recipient of the data communication (telephone numbers, IMEIs, IP addresses, MAC addresses, port numbers, IMSI identifiers, account identifiers – email, username, etc.) and for identification of the date, time, manner and duration of the communication (communications protocol details, type of communication, time and date of the communication, duration, length, etc.). To clarify (interpret) the facts relevant to the criminal proceedings it is necessary to use an expert. Such practical procedure has developed because of the actual need and possibility and the use of the expertise under Section 105 et seq. has thus proven to be currently the most available institute.

132 This opinion was confirmed by the Supreme Court. The decision of the Supreme Court, file number 5 Tdo 572/2009, No. 7/2008 Sb. tr. rozh.

7.2 Inadmissibility of evidence as a consequence of inappropriate collection

It is not permissible to exclude any type of evidence except in the cases indicated by the Section 89 of the Code of Criminal Procedure. The Code of Criminal Procedure, however, does not contain any further statement which would require explicit enumeration of all the cases of inadmissible evidence. This is why it is necessary to follow the general requirements about the admissibility of evidence in the Code of Criminal Procedure and with respect to the proceedings.[133] The inadmissibility of evidence is therefore deduced mainly from the interpretation of the provisions. There are two main approaches in the Constitutional Court regarding the inadmissibility of evidence based on whether there was any misconduct in obtaining the evidence. The first concept is based on the fact that the evidence is inadmissible because of the prohibition of arbitrariness, which sets out the obligation of the courts and other relevant authorities to not deviate in any way from the rules of procedure.[134] The second approach is based on the infringement of the right to a fair trial through a breach of the rights of another person, e.g., privacy rights.

Specific questions connected with the inadmissibility of the interception (Section 88) are described subsequently. Generally, the records of communication of a person that were acquired against the law (especially if the conditions under Section 88 were not fulfilled) are taken as absolutely inadmissible evidence. Transcripts of such recordings cannot be filed in the criminal file. If this happens, the transcript, as well as the records themselves, cannot be used in criminal proceedings as evidence.[135]

On the basis of Section 88 para. 1 (third sentence), the interception and recording of telecommunication between the defense counsel and the accused is inadmissible and it has to be destroyed. Such a prohibition does not apply, however, to the communication of the accused person with

133 It is also necessary to keep in mind the Section 8c and Section 30 paragraph 4 of the Code of Criminal Procedure.

134 Decision of the Constitutional Court file number III. ÚS 501/04, N 42/36 SbNU 445.

135 Decision of the Regional Court in České Budějovice from 29 September 1994, file number 4 To 354/94.

his/her family members.[136] It is also necessary to fully follow the conditions stipulated under Section 88 para. 6 regarding attaching the protocol containing the information specified above[137] in order to be able to use the evidence in the criminal proceeding. Only the recordings of telecommunications relevant to the case may be included in the criminal case file. Other communications discussed in Section 88 para. 6 must be protected against unauthorized use and kept outside of the criminal case file. It is especially necessary to protect personal data and third person data contained in the records which have no connection to the criminal proceedings.[138]

The interception and recording of telecommunications for the purpose of criminal proceedings is governed by the provisions of Section 88 of the Code of Criminal Procedure. This allows taking such action, also before the commencement of the prosecution, but only in the case of emergency and urgent operations. The interception can be used in criminal proceedings only if it was conducted on the basis of Section 88 of the Code of Criminal Procedure. Interception carried out under any other legal act, e.g., under Act No. 283/1991 Sb. on the Police of the Czech Republic or under Act No. 13/1993 Sb., Customs Act, can only be used for the purposes defined by these acts (the means of operative techniques). This must be respected even if the evidence was collected under the same conditions that would otherwise be sufficient to carry out urgent interception according to the Code of Criminal Procedure. The records of such an interception (and the interception itself), as well as any other operative technique materials, cannot be used as evidence.[139] It was decided previously by the European Court of Human Rights in the case of A. v. France that interference with

136 Decision of the Supreme Court, file number 4 Pzo 3/2011-37.

137 Decision of the High Court in Prague from 18 January 2001, file number 4 To 3/01.

138 Decision of the Constitutional Court file number III. ÚS 3221/09, N 197/58 SbNU 741.

139 The Act on the Police of the Czech Republic and the Customs Act have been amended, however the decision of the High Court serves as an example of narrow interpretation of the possibility to use the intercepted evidence in criminal proceedings. Decision of the High Court in Prague from 8 June 2000, file number 2 To 73/2000.

privacy in the attendance of police authorities was found to breach Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.[140]

Despite the fact that the evidence was obtained in violation of the law, such evidence may still be used in criminal proceedings. The Constitutional Court stated that in order for an audio recording recorded by a private person without the consent of the person whose voice was recorded to be used as evidence, it is necessary to consider firstly whether the evidence (e.g. an audio recording on a cell phone) of the witness stands alone in a concrete situation when evaluating the guilt of the offender, or whether the court also has other evidence at its disposal which significantly supports the merits of the accusation and which is also supported by the recording of the conversation.[141] The information contained in the recording can serve as evidence in criminal proceedings only if the invasion of privacy is justified by the overriding interests of the person who provided the information in the manner described and then used. According to the opinion of the courts, illegally taken recordings can only be used as supportive evidence to verify the facts stated in both interception and witness testimony.[142]

It is necessary to state the date after which the intercepted communication that was created in this time can be used as evidence in criminal proceedings. For example: in criminal proceedings, cell phones are treated in the same manner as any other tangible thing. The data stored on cell phones are evaluated in a similar way. The authorities in criminal proceedings can therefore extract all the data stored on the phone and such evidence can be used in criminal proceedings. But it is necessary to distinguish the specific moment at which the communication was taking place and to distinguish the use of various procedural instruments.[143] This was confirmed by the Explanatory Opinion

140 Detained suspected hitman agreed to cooperate with the police to record a phone call with suspected person to prove, that he was hired by her to commit homicide. Such evidence was found as inadmissible. A. v. France, decision from 23 November 1993, Application No. 14838/89.

141 Decision of the Constitutional Court file number II. ÚS 143/06.

142 This was confirmed by the decision of the Supreme Court, file number 5 Tdo 459/2007 or by the decision of the Supreme Court, file number 8 Tdo 908/2013.

143 Such interpretation was confirmed by the decision of the Supreme Court, file number 7 Tz 9/2000.

of the Supreme Public Prosecutor's Office No. 4/2005.[144] Following this opinion, police authorities do not need an interception order from a judge (issued on the basis of Section 88 of the Code of Criminal Procedure) if the data had already been delivered and was present on the cell phone even before the moment at which the police authority took the cell phone into its possession.[145] This means that all the data stored on the cell phone at moment of securing may be used as evidence.

In the case of uncollected voicemail, it is necessary to issue an interception order according to Section 88 of the Code of Criminal Procedure. Voicemail (unlike an unread SMS message) is not stored directly on the cell phone. Voicemail can only be collected from the data storage of a service provider through the cell phone. Such data cannot be used as evidence in the criminal proceedings on the basis of seizure of property proceedings. It was stated in the Explanatory Opinion of the Supreme Public Prosecutor's Office No. 1/2015 that it is necessary to issue an interception order prior to the commencement of the communication itself if the voicemail is planned to be used as evidence.[146]

Any communication, which is not statically stored via secured remote service or storage but is still the subject of electronic communications (email or other messenger communication services), has a special position. The Explanatory Opinion states that the provider of electronic

144 The Supreme Public Prosecutor's Office, SL 788/2004, The Collection of the Explanatory Opinions of the Supreme Public Prosecutor's Office, No. 4/2005, in Brno 6 June 2005, accessible at: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2005/stanovisko%204-2005.pdf.
This opinion also stated that the data stored in SIM card inserted in the cell phone have the same position as the data stored directly in the cell phone.

145 It is necessary to state that securing of the cell phone was issued under different provisions than the provision concerning the interception. In this case the proceedings are stated in Section 78 (Obligation to Release Property) and Section 79 (Seizure of Property) of the Code of Criminal Procedure.

146 The Supreme Public Prosecutor's Office, 1 SL 760/2014, The Collection of the Explanatory Opinions of the Supreme Public Prosecutor's Office, No. 1/2015, in Brno 26 January 2015, accessible at: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

communications is not entitled to store and transfer message content.[147] The Supreme Public Prosecutor's Office then concludes on the basis of such statement that Section 88 of the Code of Criminal Procedure can be only used for real-time communication.

If the evidence (interception) was acquired legally, it cannot be excluded by the court only because of the fact that the legal regulation on evidence proceedings has changed. The legality of such proceedings is decided on the basis of the legal regulation that was in the force at the time the measures to acquire such evidence were taken.[148]

When disclosing the committing of serious crimes, the Police can interfere in a lawful manner with different developmental stages of a criminal offense. It cannot provoke (initiate) criminal activity that would not be committed without such provocation. The opinion that the duty of the Police is always to prevent a criminal offense from being committed in its initial stage would prevent the use of operative and investigative methods (interception). This would make such methods useless and would lead to paralysis on the part of the Police and their attempts to carry out their tasks in the process of the detection of serious criminal offenses and to reveal the identity of the offender. It is also necessary to address the question of culpability in relation to the application of a higher criminal sentence when deciding whether the requirement of Section 88 para. 1[149] is fulfilled or not.[150]

From the point of view of constitutionally protected fundamental rights it cannot be possible to commence a criminal procedure using only interception to subsequently justify that serious crime (under Section 88 para. 1) was committed if such justification was based only on a speculative basis.[151] The Constitutional Court strongly stressed that if there are any specific facts

147 The Supreme Public Prosecutor's Office, 1 SL 760/2014, The Collection of the Explanatory Opinions of the Supreme Public Prosecutor's Office, No. 1/2015, in Brno 26 January 2015, accessible at: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf. P. 8.

148 Decision of the Constitutional Court file number Pl. ÚS 47/13, N 76/73 SbNU 351.

149 The interception can be used only in the case of serious crimes; thus it is necessary to assess whether such crime described in Section 88 paragraph 1 was really committed.

150 Decision of the High Court in Prague file number 2 To 139/2005.

151 Decision of the Constitutional Court file number II.ÚS 789/06, N 150/46 SbNU 489.

supporting the suspicion for committing a serious crime, then, with regard to the constitutional limits of regulation of interception, such facts have to be clearly apparent in the rationale of the interception order. The specific rationale, however, contained only very vague argumentation to support the suspicion that a person was in attendance during a particular criminal action. The interception order did not include specific facts to make it clear that a particular person was suspected of committing the criminal offense. It is necessary to use proper and persuasive argumentation in the interception order on why it was decided to use such a strong procedural instrument that interception certainly is.[152] Without a precise rationale in the interception order, the information gained on this basis cannot be used in the criminal proceedings.

The facts stated above serve as the general concept on how the limitation and consideration of the admissibility of interception as evidence works in the criminal proceedings. If the limits indicated above are exceeded, the use of interception as evidence cannot be found to be legitimate; thus, the communication data contained in the interception will be regarded as illegally obtained.

It is also necessary to respect the strictly limited range of situations when the providers of electronic communication can collect traffic and location data, which also determines the need to proportionally test the use of traffic and location data in criminal proceedings. This was also underlined by the Constitutional Court which pointed out that Section 88a para. 1 explicitly mentions the list of criminal offences under which it is possible to issue the collection of traffic and location data. In the specific decision the court stressed that if the criminal offence did not fall under these criminal offences mentioned under Section 88a para. 1, it was only possible to collect and use traffic and location data in the criminal proceedings if the condition under Section 88a para. 4 was fulfilled (the subjects themselves agreed with

152 Decision of the Constitutional Court file number II. ÚS 2806/08, N 15/56 SbNU 143.

the collection and use of such data). Any other collection of traffic and location data which does not fall under such conditions has to be seen as illegal and unusable in criminal proceedings.[153]

It is sufficient for the justification to collect traffic and location data by providers of electronic communication under Section 88a para. 1, if it is only said, that all the information concerning "all accessible emails" will be collected. As the data retention is directed only to the past (contrary to the interception), this less specific definition of the time period still has to be regarded as sufficient and in line with the requirements laid down by the Code of Criminal Procedure.[154]

7.3 Use of data outside the main proceedings

7.3.1 Data from other criminal investigations

The interception and recording of telecommunication can be used in another criminal case as evidence under the condition that:

1. in this other criminal case there is criminal prosecution for a criminal offence referred in Section 88 para. 1. These are crimes for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, for a criminal offence of machinations in insolvency proceedings, violation of regulations on the rules of competition, negotiating advantages during public procurement, tender and auction, misuse of powers of an official person or for any other intentional criminal offence, for which the prosecution is stipulated in a declared international treaty, or
2. with the consent of the user of the intercepted station (which means anyone who uses or requests a publicly available electronic communication service).[155]

153 Decision of the Constitutional Court file number III. ÚS 3844/13, N 201/75 SbNU 259.

154 Decision of the Constitutional Court file number III. ÚS 2661/12.

155 Section 88 paragraph 6. Third sentence. The Code of Criminal Procedure. The wording of Section 88 paragraph 6 was enacted in 1 July 2008, but the use of the evidence in another criminal proceedings under certain condition was already expressed in the decision of the Constitutional Court file number II. ÚS 6/93, N 22/1 SbNU 159.

It should be stated that if there was an interception order issued on the basis of committing a serious criminal offense (as stated in Section 88 para. 1), in the first case of criminal prosecution, then the fact that the criminal prosecution against the same person for another criminal offense (which was, however, not a serious criminal offense mentioned in Section 88 para. 1) was initiated after that does not mean that interception would be illegal against that person. Such interception cannot, however, be used as evidence for the second, less serious offense; it can be used to support the facts only in the first case of criminal prosecution.[156]

The requirements that have to be contained in the interception order are listed in Section 88 para. 2. *"The interception order and recording of the telecommunications service shall include a determined user address or a user device and the user if their identity is known, and the period during which the interception and recording 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."* In case of possible use of the intercepted data for the prosecution of individuals who were not the subject of the interception order, it has to be concluded that if there was already ongoing interception, evidence on the basis of such interception could also be used for the criminal offense that had been discovered during the interception. This evidence can, however, be used only if the discovered criminal offence fulfils the conditions of serious crime listed in Section 88 para. 1. If these conditions are fulfilled, then it is not relevant whether the interception was allowed and the recording acquired regarding the suspect, accused, or any other person.[157]

7.3.2 Data from preventive investigations

The case law of the European Court of Human Rights, in limiting the fundamental right to privacy for security reasons, strictly restricts the conditions for the applicability of evidence obtained by limiting privacy. It approves only such practices, which can offer adequate safeguards to protect fundamental

156 Decision of the Supreme Court file number 4 Pzo 2/2010.
157 Decision of the Supreme Court file number 2 To 144/2003.

rights e.g. against abuse or arbitrariness because, in the opposite case (and also because of the present technological possibilities), democracy itself would be at stake.[158]

Based on the above-mentioned arguments, the Constitutional Court considered the possibility of using interception outside of the criminal proceedings (intelligence service) in criminal proceedings. Interception of communication by public authorities (as well as any other type of secret surveillance) represents a serious limitation of fundamental rights. It is implied from the interception order that the limitation of personal integrity and privacy may be made by public authorities, albeit very rarely, only when necessary and if the aim of pursuing public interest cannot otherwise be achieved. Failure to comply with certain conditions means that such action is unconstitutional.

The intelligence law incorporates less limiting rules on the breach of privacy; these milder conditions are only tolerated when limited by strict intent of the use of the gathered information and also by the seriousness of the possible threat.

Using intelligence interception in criminal proceedings as evidence of guilt is not foreseen in the Code of Criminal Procedure or in the law on intelligence services. In specific cases, interceptions were acquired pursuant to the act relating to the intelligence services. The intelligence service crossed the boundaries of the law when it provided a highly concretized, extensive set of information to the authorities prosecuting a criminal offence. In relation to the criminal proceedings law, intelligence services are only entitled to provide basic and general information (Section 8 para. 3 of Act No. 153/1994 Sb. on intelligence services of the Czech Republic). Any use of interception outside of the sphere of application of the law on intelligence services was and is an ongoing violation of fundamental human rights. It was explicitly stated that the potential threat of terrorist attack also cannot breach the barrier of constitutional mechanisms.[159]

158 This principle was highlighted also in the case of Klass v. Germany (especially in the paragraphs 42, 48, 49, 50). Klass and others v. Germany, decision from 6 September 1978, Application No. 5029/71.

159 Decision of the Constitutional Court file number I. ÚS 3038/07, N 46/48 SbNU 549.

7.3.3 Data from foreign jurisdictions

The questions on acquiring, using, and admitting evidence of intercepted data from abroad are regulated mainly by Act No. 104/2013 Sb. on international judicial cooperation in criminal matters. This law deals with the issues of interception in Section 47 where the possibility to provide legal assistance to another state based on the principle of reciprocity is established. This section, however, states that it is unconditionally necessary to respect the rules incorporated in the Code of Criminal Procedure.

If an international treaty stipulates that the interception can be carried out by a foreign country on the territory of the Czech Republic without the technical assistance of the Czech Republic, the Regional Court in Prague is responsible for deciding on the consent to interception or its continuation; if a preliminary procedure is conducted in the foreign state, which will perform the interception, the Public Prosecutor from the Regional Prosecutor's Office in Prague decides on the admissibility of such interception. The consent to interception or its continuation can be granted only if the conditions set out in Section 88 of the Code of Criminal Procedure are completely fulfilled.[160] The general rule to respect the requirements under Section 88 of the Code of Criminal Procedure has also been highlighted by the Supreme Court in the past and before Act No. 104/2013 Sb. on international judicial cooperation in criminal matters was in force. It was also stressed that it is necessary to rationalize any intervention into privacy.[161]

If an international treaty stipulates that it is possible to carry out the interception of telecommunication from the Czech Republic on the territory of a foreign state without its technical assistance, the prosecutor and – after filing the indictment – the court informs the foreign state about the anticipated interception in the manner provided by that international treaty.[162]

160 Section 64 paragraph 1. Act No. 104/2013 Sb., on international judicial cooperation in criminal matters.

161 The decision of the Supreme Court file number 11 Tz 129/2006.

162 Section 64 paragraph 2. Act No. 104/2013 Sb., on international judicial cooperation in criminal matters.

7.4 Challenging the probity of intercepted data

According to Section 88 para. 8 of the Code on Criminal Procedure, after the criminal case becomes final, the prosecutor or the presiding judge of the court of first instance informs the person who is the user of the device about the interception order and the recording of telecommunication, unless exceptions under Section 88 para. 9 are fulfilled. Such person may submit a proposal to review the legality of the interception to the Supreme Court within six months under Section 314 l to Section 314 n of the Code of Criminal Procedure. This decision is not subject to appeal.

The prerequisite for filing a petition for review of the legality of interception in accordance with Section 314 l of the Code of Criminal Procedure to the Supreme Court is that the case was ended accordingly to Section 88 para. 8. It is also necessary that the presiding judge of the court of first instance or the prosecutor subsequently inform the person authorized to file such petition about the ordered interception. A proposal to review the legality of interception cannot therefore be submitted to the Supreme Court before the relevant case is final and without the subsequent sending of the information to the authorized person. If such a petition is filed, even if the above stated conditions were not fulfilled, the Supreme Court rejects it as inadmissible.[163]

In accordance with Section 314 l et seq. of the Code of Criminal Procedure, in the procedure for a review of an interception order, review by the Supreme Court is limited only to the assessment of legality of the issued interception order and the recording of telecommunication. Therefore, in these proceedings, the Supreme Court cannot deal with e.g. any objection related to the performance of duties of the police authority in accordance with Section 88 para. 3 or objections against the evaluation of the results of the interception directed against the rationale of the court, which decided such interception.[164]

Under the conditions of Section 88 para. 1, 2, it is also exceptionally possible to order the interception during the phase of enforcement

163 The decision of the Supreme Court file number 4 Pzo 1/2010.
164 The decision of the Supreme Court file number 4 Pzo 2/2010.

proceedings in connection with the search of a convicted person who is meant to be imprisoned for the offence listed in Section 88 para. 1. It is, however, permitted to use the interception only when any other procedures for locating such a person have failed. The legality of such interception can also be examined by means of the procedure described under Section 314 l to Section 314 n.[165]

165 The decision of the Supreme Court file number Tpjn 304/2012, No. 54/2013 Sb. Tr. Rozh.

8 DIFFERENTIAL COMPARATIVE NOTE: SLOVAKIA

8.1 Security Architecture and the Interception of Telecommunication

8.1.1 National Security architecture – Two Frameworks of Interception

It can be said that Slovak Republic legislators have been inspired in many situations by the Czech legal setting. To define the constitutional limits of interception, we have to look at the Slovak Constitution (Act No. 460/1992 Zb. Constitution of the Slovak Republic). It states in Article 2, Paragraph 3 that state bodies can act only on the basis of the Constitution, within its limits, and to the extent and in a manner defined by law. Pursuant to Article 19, everybody has the right to protection against unjustified interference with his or her private and family life and against the unjustified collection, publication, or other misuse of personal data. Article 22 guarantees the secrecy of correspondence, other communications, and written messages delivered by post, and of personal information. The privacy of letters, other communications, and written messages kept privately or delivered by post or otherwise, including communications made by telephone, telegraph and other means, cannot be violated by anyone except in cases specified by law.[166] Therefore, all the public authorities which are authorised to conduct interceptions of telecommunication fall within the scope of these articles. They are permitted to act only within what is expressly allowed to them by law.

There are two situations under which electronic communication can be intercepted. The first is the state of criminal procedure pursuant to Act No. 301/2005 in the Code on Criminal Trial (Code of Criminal Procedure). It is conducted by police forces or the court (comparable to the Czech

166 Act No. 460/1992 Zb. Constitution of the Slovak Republic. English translation taken from the webpage of the Slovak Public Defender of rights. Unofficial translation. Online: http://www.vop.gov.sk/constitution-of-the-slovak-republic.

procedure), to which a special regime of customs service can be included. According to the Code of Criminal Procedure, the order to intercept and record telecommunications can be issued by the presiding judge of a panel prior to the commencement of criminal prosecution, or by a judge for pre-trial proceedings after a motion from a prosecutor. If the matter cannot be delayed and a prior order from a judge for pre-trial proceedings cannot be obtained, the order may be issued by a prosecutor before the commencement of criminal prosecution or in pre-trial proceedings, unless the interception and recording of telecommunications involves the entry into the dwelling of a person; such an order must be confirmed by a judge for pre-trial proceedings within 24 hours of its issuance; failing that, the order shall become null and void and the information obtained on its basis may not be used for the purposes of criminal proceedings and shall have to be immediately destroyed in a prescribed manner.[167]

The second situation is for civil and military intelligence services (regulated by Act No. 46/1993 Zb. in the Slovak Information Service and Act No. 198/1994 Zb. on Military Intelligence) and other entitled authorities (Police Corps, Prison and Court Guard, and the Customs).

The difference between Slovak and Czech legislation is reflected in Act No. 166/2003 Zb. on the Protection of Privacy against Unauthorised Use of Information-technical Means amending and supplementing certain acts (Act on the Protection against Interception). This Law specifies the conditions required for the use of technical-intelligence measures without the prior consent of the person whose privacy is infringed upon by the state body which is using the intelligence-technical measures (ITM). This Law does not apply to the use of ITM in a criminal proceeding in accordance with a specific law (Code of Criminal Procedure).[168] However, there are notable exceptions. The ITM can be used by the Police Corps, the Slovak Information Service, Military Intelligence, the Railway Police, the Corps of Prison and

167 Section 115 para.1 of No. 301/2005 Zb. Code of Criminal Procedure. The European e-Justice Portal. Unofficial translation. Online: https://e-justice.europa.eu/fileDownload.do?id=11f9da19-253e-4f02-9a26-2e2285184e7a.

168 Section 1 of Act No. 166/2003 on the Protection of Privacy against Unauthorised Use of Information-technical Means amending and supplementing certain Acts (Act on the Protection against Interception). Unofficial translation. Online: http://www.sis.gov.sk/files/zakony/act_166_2003.pdf.

Judiciary Guards, and the Customs Board in the extent pursuant to specific regulations. The execution of ITM for all authorities is technically provided by the Police Corps following the submission of a written approval of the legitimate. Generally, ITM can be used only if it is "*required in a democratic society to safeguard the security and defence of the country, to prevent and reveal criminal activities, or to protect the rights and freedoms of other persons*."[169] An additional general principle is that by using ITM the essential right or freedom can be infringed upon only to the required extent and for a period of time not longer than inevitable to attain the legal goal, to which it serves.

The Slovak Information Service is authorised to use these means in order to carry out its legal tasks. These means can be utilised to infringe the privacy of persons without their prior approval in accordance with the conditions stated in the law. Also, they can be utilised upon the prior approval of a judge. It is possible to utilise ITM for a period of no more than 6 months. This period starts upon the day the approval is granted. If it is necessary to utilise several types of ITM, either at once or subsequently, each ITM can only be utilised in the scope approved. If ITM are to be utilised in places not accessible to the general public, the judge granting the approval decides whether approval is also given for entering such places.[170]

Moreover, the Act on the Protection against Interception brings distributive option of interlining the two regimes (intelligence and criminal procedure). In an exceptional case, if there is reasonable suspicion of a crime being committed and ITM might be used, the Police Corps (or investigation authorities) may use ITM even without a prior approval of a legitimate judge. The case must be dealt with immediately and the approval of the legitimate judge cannot be obtained in advance. Even the Police Corps are required to notify a legitimate judge of the use of the ITM within one hour of the beginning of the use of this measure, stating that they are exceeding their power based upon the Code of Criminal Procedure. The legal guarantee is that if the Police Corps does not obtain subsequent written approval from the legitimate judge within twelve hours from the beginning

169 Section 20 of Act on the Protection against Interception.

170 Slovak Information Service: Annual Report 2013. Online: http://www.sis.gov.sk/for-you/sis-annual-report-2013.html.

of the use of the ITM or if the legitimate judge does not grant the subsequent approval, the use of this measure shall be immediately ceased, and moreover, information obtained in this way shall not be used and it shall be immediately destroyed. The state body, which has destroyed this information, shall immediately notify the legitimate judge of the destruction.[171]

The Act on the Protection against Interception serves not only as the base for legal intelligence interception but it opens doors to using the obtained evidences in criminal procedure.[172] This is subject to expected judicature of higher courts, therefore, the separation of two spheres is not very clear here and intelligence legislation is interrelated with criminal procedure in some cases. Even more, it passes specific power to police authorities, which are entitled under former intelligence legislation and certain circumstances to intercept without court approval, which might raise some constitutional questions.

8.1.2 Legislative grounds

The communication interception in the criminal procedure is regulated in the Section 115 of the Code of Criminal Procedure: [173]

> *"Interception and recording of telecommunications*
>
> *Section 115*
>
> *(1) Where criminal proceedings are conducted in respect of a felony, corruption, criminal offence of the abuse of power of a public official, criminal offence of laundering the proceeds of crime, or in respect of an intentional criminal offence where so provided by a promulgated international treaty, it shall be possible to issue an order to intercept and record telecommunications if there are reasonable grounds to believe that it will reveal the facts that are materially relevant for criminal proceedings. Where, in the course of intercepting and recording telecommunications, the accused is found to be in communication with his defence counsel, no information thus obtained may be used for the purposes of criminal proceedings, and any such information must be forthwith destroyed in a prescribed manner; this shall not apply to information relating to a case in which a lawyer does not represent the accused as his defence counsel.*

171 Section 5 of Act on the Protection against Interception.
172 Section 7 para. 2 of Act on the Protection against Interception.
173 Section 115 of No. 301/2005 Zb. Code of Criminal Procedure. Unofficial translation. Online: https://e-justice.europa.eu/fileDownload.do?id=11f9da19-253e-4f02-9a26-2e2285184e7a.

(2) The order to intercept and record telecommunications shall be issued by the presiding judge of a panel prior to the commencement of criminal prosecution, or by a judge for pre-trial proceedings on a motion from a prosecutor. If the matter bears no delay and a prior order from a judge for pre-trial proceedings cannot be obtained, the order may be issued by a prosecutor before the commencement of criminal prosecution or in pre-trial proceedings, unless the interception and recording of telecommunications involves the entry into the dwelling of a person; such order shall have to be confirmed by a judge for pre-trial proceedings within 24 hours of its issuance; failing that, the order shall become null and void and the information obtained on its basis may not be used for the purposes of criminal proceedings and shall have to be immediately destroyed in a prescribed manner.

(3) The order to intercept and record telecommunications shall have to be in writing and based on circumstantial reasons, separately for each telephone subscriber or piece of technical equipment. The order shall have to specify the telephone subscriber or piece of technical equipment and, if known, the person whose telecommunications are intercepted and recorded, and the length of time during which the interception and recording of telecommunications is to be performed. Interception and recording may not exceed six months. This period may be extended by another two months, also repeatedly, by a motion from a prosecutor or a judge for pre-trial proceedings. Interception and recording of telecommunications operations shall be performed by a competent department of the Police Corps.

(4) Police officers or a competent department of the Police Corps shall be obliged to continuously review the grounds for the order to intercept and record telecommunications. Where such grounds cease to exist, interception and recording of telecommunications shall have to be discontinued, even before the expiry of the time limit referred to in paragraph 3. This fact shall be immediately notified in writing to the entity that issued the order to intercept and record telecommunications; in pre-trial proceedings, it shall also be notified to the prosecutor.

(5) In criminal proceedings conducted in respect of an intentional criminal offence which is different from the one referred to in paragraph 1, the order to intercept and record telecommunications may be issued by the presiding judge of a panel or, prior to the commencement of prosecution or in pre- trial proceedings, by a judge for pre-trial proceedings acting on a motion from a prosecutor, but only with the consent of the subscriber to the telecommunication equipment subjected to interception or recording.

(6) If the record of telecommunications is to be used as evidence, a verbatim transcript made by the officer of the Police Corps carrying out the interception

of telecommunications shall have to be attached, wherever the recording makes it possible, containing information about the place, time and legal grounds for interception. A verbatim transcript of the record of telecommunications, which is not secret, signed by the Police Corps officer who drew it up, shall be inserted in the file; if the verbatim transcript of telecommunication records contains a classified fact, it shall be classified according to separate legal provisions. The transcript of telecommunications shall be used as evidence after the interception of telecommunications has been discontinued. In pre-trial proceedings, where the circumstances of the case warrant it, the recording of telecommunications may be submitted to the court even without a transcript of the recording, if the accompanying report gives the data concerning the time, place and legality of interception, and concerning the persons subject to the recording of telecommunications, provided that the recording of telecommunications is intelligible.

(7) The recording may be used as evidence in a different criminal matter from the one that is subject to interception and recording of telecommunications only if such other matter is also heard in simultaneous proceedings concerning the criminal offence referred to in paragraph 1.

(8) If the interception and recording did not produce any facts relevant for criminal proceedings, the criminal procedure authority or the relevant department of the Police Corps shall have to destroy the obtained records forthwith in a prescribed manner. The protocol on the destruction of the recordings shall be inserted in the file.

(9) The destruction of the recordings shall be notified to persons referred to in paragraph 3 who do not have the right to view the file; the notification shall be made by the body whose decision has finally settled the matter, or, in the proceedings before the court, by the presiding judge of a panel of a first-instance court within three years from the date on which criminal prosecution in the case was finally concluded; this shall not apply to the proceedings concerning particularly serious felonies or the felonies committed by organised groups, criminal groups or terrorist groups, or criminal offences committed by more than one person if at least one of the perpetrators is still under prosecution, or if the provision of such information could obstruct the purpose of criminal proceedings.

(10) The presiding judge of a panel, police officer or prosecutor shall not provide the information pursuant to paragraph 9 in the case of a person who has the opportunity to inspect the file under this Act, or the proceedings of a particularly serious crime or a crime committed by an organized group, a criminal

organization or terrorist group, or if the crime is conducted by more people and in relation to at least one of them has been not legally ended prosecution, or where the provision of such information could defeat the purpose of criminal proceedings.
(11) The provisions of paragraphs 1 to 10 shall apply, as appropriate, to the content data or operational data transmitted in real time via computer systems."

The intercepted communication and recordings can be used for the sake of criminal proceedings only when the proceeding is conducted for crimes specifically enumerated by the law. The general rule is that the interception must be initially authorised by a judge. A comparable provision relates to creating visual, audio or audio-visual recordings pursuant to the Section 114 of the Code of Criminal Procedure. It is concentrated more on local area monitoring and wiretapping than telecommunication interception. It is used in intentional crimes only, where the maximum level of penalty exceeds 3 years in prison, corruption, abuse of the power by public officer, money laundering or another crime recognized by mutual legal assistance.

The data retention (traffic and location data) by providers of electronic communication and possibilities of accessing such data in the criminal proceedings by the Police Corps are laid down in section 116 of the Code of Criminal Procedure. The Slovak Constitutional Court has recently held this provision as unconstitutional.[174]

"Section 116
(1) In criminal proceedings held in respect of an intentional criminal offence, it will be possible to issue an order for the disclosure and provision of telecommunications data that are subject to telecommunications secrecy or enjoy personal data protection, if such data are necessary to clarify the facts relevant for criminal proceedings.
(2) The order to disclose and provide telecommunications data shall be issued in writing by the presiding judge of a panel prior to the commencement of criminal prosecution, or by a judge for pre- trial proceedings on a motion from a prosecutor in pre-trial proceedings, which must be based on circumstantial reasons; the order shall be served on the persons referred to in paragraph 3.

174 Press news of Slovak Constitutional Court from April 29, 2015. sp. zn. PL. ÚS 32/2015. Translation of author. Online: https://www.ustavnysud.sk/docDownload/b6cd9bed-c37c-4d6c-a8c3-bf92046e7296/č. %2052%20-%20PL.%20ÚS%2032_2015.pdf.

> *(3) Legal entities or natural persons carrying out telecommunications activities shall notify the presiding judge of a panel, or, in pre-trial proceedings, a prosecutor or a police officer about effected telecommunications.*
>
> *(4) The provisions of paragraphs 1 to 3 shall apply, as appropriate, to the content data or operational data transmitted in real time via computer systems.*
>
> *(5) The prosecutor shall not provide the information pursuant to paragraph 4 in the case of a person who has the opportunity to inspect the file under this Act, or the proceedings of a particularly serious crime or a crime committed by an organized group, a criminal organization or terrorist group, or if the crime is conducted by more people and in relation to at least one of them has been not legally ended prosecution, or where the provision of such information could defeat the purpose of criminal proceedings.*
>
> *(6) The provisions of paragraphs 1 to 5 shall apply, as appropriate, to the content data or operational data transmitted in real time via computer systems."* [175]

Relating to this obligation, the providers of electronic communications were obliged to store traffic data, location data and data about the communicating parties for a period of six months (in the case of Internet, email or VoIP communications) or for a period of 12 months (in case of other communications). It was held that the legal framework regulating the access to data retention data was completely arbitrary and considerably less stringent than comparable provisions on wire-tapping.[176]

Also, strong powers arise from Act No. 171/1993 Zb. on the Police Corps. Police Corps can use ITM and conclude operative-investigative activities in performing tasks in the fight against terrorism, the fight against money laundering, narcotics, nuclear materials, and forgery. Also, ITM are used in assistance to exposed witnesses and in the witness protection program under special regulation. Another option is the protection of an agent in detecting tax evasion and illicit financial activities. The scope of the police corps competence regarding interception is quite broad. According to the European

175 Section 116 of No. 301/2005 Zb. Code of Criminal Procedure. Unofficial translation. Online: https://e-justice.europa.eu/fileDownload.do?id=11f9da19-253e-4f02-9a26-2e2285184e7a.

176 The decision was issued almost a year after the CJEU proclaimed the Data Retention Directive invalid in the spring of 2014. See Slovakia: Gera, M. Mass surveillance of citizens is unconstitutional. Protecting digital freedom. *EDRi.org*. May 4, 2015. Online: https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/.

case law, and also according to the national one, the police cannot use ITM in a case of intercepting a communication between client and attorney (e.g., a similar concept to the attorney client privilege). The attorney client privilege is recognized in criminal or public law matters only (the antitrust and competition practice recognize a similar concept as well).

According to the Act on the Protection against Interception, ITM is primarily electro-technical, radio-technical, photo-technical, optical, mechanical, chemical, and other technical measures and equipment or their sets, used in a covert manner in: searching for, opening, examination, and assessment of mail and other transported packages, monitoring and recording of telecommunication activities, and making and using visual, audio, and other recordings.[177] The most important provision for the Slovak Intelligence Service and other authorities empowered to interception activities arises from following provision of the Act on the Protection against Interception:[178]

> *"Section 4*
>
> *(1) Technical-intelligence measures shall be used only on the basis of the prior written approval of a legitimate judge*[179] *(hereinafter "approval") and only for a set period of time, not exceeding six months. The term shall go into effect on the day the approval is granted. If it is necessary to simultaneously or subsequently use several kinds of technical-intelligence measures, each of them shall be used only to the extent of the expressly granted approval. If the technical-intelligence measure is to be used in places, which are not accessible to the public, the legitimate judge shall also decide whether his approval applies also to the entry into such places.*
>
> *(2) The legitimate judge who has granted the approval to use the technical-intelligence measures can, on the basis of a new request, extend the duration of the time period, but in each case for no longer than other six months. This term shall go into effect on the day the further approval is granted (hereinafter "further approval"). Further approval shall be granted in writing not later than on the last*

177 Article 2 of Act on the Protection against Interception.

178 Act on the Protection against Interception.

179 Article 13, Section 2 and 3, and Article 20, Section 2 of the Law of the Slovak National Council No. 335/1991 in the Code on the Courts and Judges, as stated in Article III of the Law No. 185/2002 in the Code on the Judicial Council of the Slovak Republic and on the Amendment and Supplementation of Some Laws.

day of the term in accordance with paragraph 1. If the term cited in paragraph 1 expires and the further approval is not granted, the use of the technical-intelligence measure shall be ceased on the last day of the term set in the approval.

(3) The request to grant approval to use a technical-intelligence measure (hereinafter "the request") shall be submitted in writing to the competent court. The request shall contain the following data:

a) Specification of the type of the technical-intelligence measure to be used and of the location of its use, the proposed time of duration of its use, data on the person against whom the use of this technical-intelligence measure is directed,

b) Information on the previous ineffectual or considerably difficult revelation and documentation of activities, which constitute the reason for submitting the request,

c) The rationale for using the technical-intelligence measure. The court must not make a decision on a request which does not contain the data required by the law. It shall return the request to the applicant.

(4) The request is submitted by the state body which intends to use a technical-intelligence measure to implement its legitimate activities (Section 2, paragraph 2).

(5) It is not possible to lodge a legal remedy against the decision on approval.

(6) The legitimate judge who has granted the approval to use the technical-intelligence measures shall be required to review systematically the existing rationale of their use. If the rationale no longer applies, he shall be required to issue a decree immediately that the use of these measures cease.

Section 5

(1) In an exceptional case, if there is reasonable suspicion of a crime being committed and a technical- intelligence measure might be used by the Police Corps to fulfil its tasks, if the case is to be dealt with immediately and the approval of a legitimate judge cannot be obtained in advance, the Police Corps may use a technical-intelligence measure even without a prior approval. The Police Corps shall be required to notify a legitimate judge of the use of the technical-intelligence measure within one hour from the beginning of the use of this measure, and to submit the request in accordance with Section 4, para. 3, to the legitimate judge within six hours from the beginning of the use of the technical-intelligence measure. The request shall also contain the time datum of the beginning of the use of the technical-intelligence measure.

(2) If the Police Corps does not obtain a subsequent written approval of a legitimate judge within twelve hours from the beginning of the use of the technical-intelligence measure or if the legitimate judge does not grant the subsequent approval,

the use of this measure shall be immediately ceased. Information obtained in this way shall not be used and it shall be immediately destroyed. The state body, which has destroyed this information, shall immediately notify the legitimate judge of the destruction."

As mentioned above, Slovak regulation for intelligence services, which is also broadly used by police authorities, has lower legal prerequisites than the Code of Criminal Procedure. Judge approval as a guarantee of lawful process is sometimes omitted due the faster and flexible investigative reactions to dangerous forms of criminality. On another hand, these powers shall be controlled and supervised by judicial power only, because they can represent misbalance or a potential risk of abuse.

8.1.3 Responsibility for the technical performance and legitimacy of data transfers between different security services

In the Slovak Republic, the technical implementation of the communication interception is done by the state/public authorities (police corps or intelligence service) with cooperation of compliant subjects pursuant to the Act No. 351/2011 Zb. on electronic communication. Section 63 Paragraph 7 of the Electronic communication act establishes a duty for a provider of a public communications network or a publicly available electronic communications service to provide and secure interfaces at specified points of the network for connection of terminal equipment for message tapping and recording (e.g., wiretapping).

The legitimacy of data transfers between various security services in The Slovak Republic is a subject of current legal discussion. Even the authorities do not hold the legitimization to intercept for the preventive purposes, there is no clear separation line between criminal and intelligence procedures. The above-mentioned Act on the Protection against Interception empowers legal interception to both bodies. The general rule is that the copy of intercepted data (electronic evidence), which has been made using ITM, can be released only to the case-related and locally authorized state body if the copy can serve as evidence in a procedure lead before the authorized state body within the limits of its authority established by the law. The case-related and locally authorized state body, to which the recording has been

released, is allowed neither to make a copy of the recording nor to release its transcription for inspection or copying to another person, to another state body or to a body of the local government or of other self-administration. The regulation is missing interpretation of what is "a case-related and locally authorized state body". This question must be decided by future case law.

8.1.4 Statistics on Telecommunication Interception

Slovak Intelligence Service (2014 – recent data)[180]

Slovak Intelligence Service in 2013 submitted 235 requests to use ITM; the court issued 230 approvals; 5 requests were rejected. Out of 230 uses of information-technical means, all cases were evaluated in terms of aims and purposes as stated by law. The aims and purposes as defined by law were reached in 217 uses of information-technical means; in 13 cases they were not. In 2013, upon requests by SIS, 187 court rulings on providing the subject of telecommunication secrecy were issued that included lists of data of communicating parties (billing), locations and additional operational data relating to users of telecommunication services.

	Section 2(1(a))	Section 2(1(b))	Section 2(1(c))	Total
Number of ITM request - Section 4 (1)	0	206	29	235
Court Approvals	0	202	28	230
Rejected	0	4	1	5
Number of ITM renewal requests to prolong the period of ITM use within the same case – Section 4 (2)	0	0	0	0
Court Approvals	0	0	0	0
Rejected	0	0	0	0
Number of ITM uses that reached aims and purposes as stated by law	0	191	26	217

180 Slovak Intelligence Service. Annual Report. Online: http://www.sis.gov.sk/for-you/sis-annual-report.html.

Number of ITM uses that did not reach aims and purposes as stated by law	0	11	2	13
Number of ITM uses where information was used as evidence in criminal proceedings	-	-	-	-
Number of illegitimate ITM uses	0	0	0	0

According to the 2014 statistics, the Slovak Information Service submitted 256 requests to use ITM, 13 requests were rejected. Out of 230 uses of ITM, the aims and purposes as defined by law were reached in 237 uses of information-technical means; in 6 cases they were not. In 2014, there were 57 requests approved to collect information containing telecommunication secrecy initiated by SIS and forwarded to the District Court in Bratislava and none were rejected.

General Prosecution of Slovak Republic (2014 – recent data)[181]

		2013	2012	2011
Producing video, audio or visual-audio recordings (Section 114 of The Code of Criminal Procedure)	Number of requests	70	103	96
	Court approvals	62	99	95
The interception and data retention (Sections 115 and 116 of The Code of Criminal Procedure)	Number of requests	4395	3459	2576
	Court approvals	3700	2826	2327

According to the 2014 statistics, activities of the Office of the Special Prosecutor were characterized by a rich use of ITM by tapping and recording telecommunications in accordance with Section 115 of the Criminal

181 General Prosecution of Slovak Republic. Annual Report 2013. Online: http://www.genpro.gov.sk/spravy-o-cinnosti-12b7.html.

Procedure Code. It must be said that the judges of the specialised criminal court refused to permit the use of the facility in 95 cases. Also, there is an increasing number of cases where accused persons attack the authenticity of the evidence. Therefore, the importance of the forensic examination of such records is very important. However, the problem is usually obtaining the voice samples of the accused persons. The law does not lay any obligation on persons to provide such samples.

Police Corps (2014 – recent data)[182]

	Section 2(1(a))	Section 2(1(b))	Section 2(1(c))	Total
Number of ITM request - Section 4 (1)	-	1165	61	1226
Court Approvals	-	1089	57	1146
Rejected	-	76	4	80
Number of ITM renewal requests to prolong the period of ITM use within the same case – Section 4 (2)	-	148	10	158
Court Approvals	-	134	10	144
Rejected	-	14	-	14
Number of ITM uses that reached aims and purposes as stated by law	-	1058	62	1120
Number of ITM uses that did not reach aims and purposes as stated by law	-	165	5	170
Number of ITM uses where information was used as evidence in criminal proceedings	-	110	9	119

182 Parliamentary Committee for Defense and Security. Annual Report 2013. Online: http://www.nrsr.sk/dl/Browser/Committee?committeeExternalId=125.

Number of illegitimate ITM uses	-	-	-	-

Military Intelligence (2014 – recent data)[183]

	Section 2(1(a))	Section 2(1(b))	Section 2(1(c))	Total
Number of ITM request - Section 4 (1)	0	25	1	26
Court Approvals	0	23	1	24
Rejected	0	2	0	2
Number of ITM renewal requests to prolong the period of ITM use within the same case – Section 4 (2)	0	17	0	17
Court Approvals	0	17	0	17
Rejected	0	0	0	0
Number of ITM uses that reached aims and purposes as stated by law	0	40	1	41
Number of ITM uses that did not reach aims and purposes as stated by law	0	2	0	2
Number of ITM uses where information was used as evidence in criminal proceedings	0	0	0	0
Number of illegitimate ITM uses	-	-	-	-

Custom Board (2014 – recent data)[184]

183 Parliamentary Committee for Defence and Security. Annual Report 2013. Online: http://www.nrsr.sk/dl/Browser/Committee?committeeExternalId=125.

184 Parliamentary Committee for Defence and Security. Annual Report 2013. Online: http://www.nrsr.sk/dl/Browser/Committee?committeeExternalId=125.

	Section 2(1(a))	Section 2(1(b))	Section 2(1(c))	Total
Number of ITM request - Section 4 (1)	0	155	0	155
Court Approvals	0	141	0	141
Rejected	0	14	0	14
Number of ITM renewal requests to prolong the period of ITM use within the same case – Section 4 (2)	0	14	0	14
Court Approvals	0	13	0	13
Rejected	0	1	0	1
Number of ITM uses that reached aims and purposes as stated by law	0	150	1	150
Number of ITM uses that did not reach aims and purposes as stated by law	0	2	0	2
Number of ITM uses where information was used as evidence in criminal proceedings	0	5	0	5
Number of illegitimate ITM uses	-	-	-	-

8.2 Constitutional Safeguards of Telecommunication

8.2.1 Areas of constitutional protection

Areas of constitutional protection in the Slovak Republic have the same principles, background and roots as those in the Czech law system. The written Constitution, along with other documents, forms the Slovak constitutional law. The Charter of Fundamental Rights and Freedoms (Act No. 23/1991 Zb.) is identical to the Czech Charter. Therefore, basic safeguards for the protection of fundamental rights are laid down in an identical document and they are also reflected in the text of the Constitution (Act No.460/1992 Zb.).

Selected articles of the Slovak Constitution (covered also by The Charter of Fundamental Rights and Freedoms): [185]

> *"Article 16*
>
> *(1) The inviolability of the person and its privacy is guaranteed. It may be limited only in cases laid down by law.*
>
> *(2) No one may be tortured, or subjected to cruel, inhuman, or humiliating treatment or punishment.*
>
> *Article 20*
>
> *(1) Everyone has the right to own property. The ownership right of all owners has the same legal content and protection. Inheritance is guaranteed.*
>
> *(2) The law shall lay down which property, other than property specified in Article 4 of this Constitution, necessary to ensure the needs of society, the development of the national economy and public interest, may be owned only by the state, municipality, or designated legal persons. The law may also lay down that certain things may be owned only by citizens or legal persons resident in the Slovak Republic.*
>
> *(3) Ownership is binding. It may not be misused to the detriment of the rights of others, or in contravention with general interests protected by law. The exercising of the ownership right may not harm human health, nature, cultural monuments and the environment beyond limits laid down by law.*

185 Ibid. The Constitution of Slovak Republic.

(4) Expropriation or enforced restriction of the ownership right is possible only to the necessary extent and in the public interest, on the basis of law and for adequate compensation.

Article 22

(1) Secrecy of letters, other communications and written messages delivered by post and personal information shall be guaranteed.

(2) No one may violate the privacy of letters and the secrecy of other written documents and records, whether they are kept in privacy, or sent by mail or in any other way, with the exception of cases which shall be laid down by law. Equally guaranteed is the secrecy of messages conveyed by telephone, telegraph, or other similar means.

(2) No one may violate the privacy of letters and the secrecy of other written documents and records, whether they are kept in privacy, or sent by mail or in any other way, with the exception of cases which shall be laid down by law. Equally guaranteed is the secrecy of messages conveyed by telephone, telegraph, or other similar means."

The secrecy of telecommunication is recognized as a fundamental right in Article 22 of the Constitution and Article 13 of the Charter of Fundamental Rights and Freedoms. The written Constitution and Charter do not recognize the confidentiality and integrity of information systems. However, it can be interpreted from a more general fundamental right, e.g., the general protection of property coded in Article 20 of the Constitution or Article 11 Paragraph 1 of the Charter. Theoretically, the protection of information self-determination could serve as a constitutional basis for the protection of cyber security. Unfortunately, a cyber security law for Slovakia is currently in process with the outcome as yet unknown. But it is highly probable that the main legislative works on this legislative document will be inspired by Czech law.[186] Also, the same situation can be identified with the term "privacy". The term "privacy" is used in Slovak law with two main meanings. One of them denotes a general constitutional principle; another meaning of the term "privacy" (*súkromie*) arises

186 The Concept of Cybersecurity in Slovak Republic. Government materials. Online: https://lt.justice.gov.sk/Attachment/Vlastný%20materiál_docx.pdf?instEID=-1 & attEID=75645&docEID=413095&matEID=7996&langEID=1&tStamp=20150218154455240.

from the Civil Code (Act No. 40/1964 Zb.) and it establishes civil remedies for cases of infringement:[187]

> *"Protection of personhood*
>
> *Section 11*
>
> *An individual shall have the right to protection of his or her personhood, in particular of his or her life and health, civic honour and human dignity as well as of its privacy, name and expressions of personal nature."*

Finally, neither the Constitution nor the Charter explicitly defines the right to informational self-determination. Also, the Slovak Constitutional Court has not yet answered this question. Only academic works and law literature are currently arguing about the interpretation of this concept.

8.2.2 Proportionality of access to data

The doctrine of proportionality has been recognised by the Slovak Republic, which was inspired by Czech and German constitutional judicature. It is now applied by Slovak Constitutional court, and very irregularly by regular courts and even by administrative authorities. The methodological grounds of the concept of proportionality were explained in a decision of the Constitutional Court No. II. ÚS 152/08 (unofficial translation):[188]

> *"The proportionality test is typically based on the following three steps. The first step (A) is a sufficiently important objective test (test of Legitimate aim / effect), accordingly the test of the suitability (Geeignetheit) or if an action aims toward the goal which is enough important to justify intervention; the test of rational links between intrusion and intervention (authority order) and said methods (restricting the freedom of expression), if it is possible to achieve an acceptable target (the preservation of the personal honour).*
>
> *The second step (B) is the necessity test. It is the test of the necessity of the used methods for the intrusion (Erforderlichkeit, necessity of the test, a test of subsidiarity), if there couldn't be used more moderate actions.*
>
> *Finally, the third step (C) is the proportionality test in stricto sensu (Angemessenheit test of proportionality in the strict sense, proporcionate effect), which includes both (C1) practical concordance (practical conformity), i.e. the test of preserving*

187 Act No. 40/1964 Zb. - The Civil Code. Unofficial translation. Online: http://ceflonline.net/wp-content/uploads/Slovakia-Property-Relations.pdf.

188 Decision of the Slovak Constitutional Court No. II. ÚS 152/08. Translation of author. Online: http://portal.concourt.sk/.

> *a maximum of both fundamental rights and (C2) called Alexy's weighing formula. An example of practical conformity could be a situation where the community, instead of banning a meeting because another meeting is held at the same time and place, involves the police to conduct both meetings. […] Weighing formula works with a three-level scale of values: "low", "medium" and "substantial". The intensity of intrusion to one of the fundamental right competes with the degree of the satisfaction rate of the second law in a collision. The intensity of intrusion and the degree of satisfaction have one of values-such as "low", "medium" and "substantial"."*

The test has not been used regarding electronic evidence or intrusions into information systems in any notable case yet (usually it is used with the preservation of personal honour, general publishing law, real estate law[189] or in a case regarding health insurance and profit[190]). One interesting case before the Constitutional Court regarding wiretapping has brought minor explanation over the doctrine of proportionality, where the court noted:

> *"Finally, the proportionality of the intrusion means that the intrusion can be executed only when it is necessary (the aim can not be achieved by moderate methods) and only in the spirit of the requirements placed on the democratic society of pluralism, tolerance and free spirit. […] The issuance of the order for the interception requires specific relevant explanatory argument, by which facts would fulfil the conditions laid down by law for the infringement of the right to privacy. The order or an approval can not be subject to review without such a reasoning relying on the specific facts."*[191]

Finally, on April 29 2015, the Constitutional Court of the Slovak Republic ruled that the mass surveillance of citizens is unconstitutional. The decision was made in the context of proceedings initiated by 30 Members of Parliament on behalf of the European Information Society Institute, a Slovakia-based think-tank. *"According to now invalid provisions of the Electronic Communications Act, the providers of electronic communications were obliged to store traffic data, location data and data about the communicating parties for a period of six months*

189 Decision of the Slovak Constitutional Court No. PL. ÚS 3/00. Online: http://portal.concourt.sk/.

190 Decision of the Slovak Constitutional Court No. Pl. ÚS 3/09. Online: http://portal.concourt.sk/.

191 Decision of the Slovak Constitutional Court No. I. ÚS 114/2012. (informal translation). Online: http://portal.concourt.sk/Zbierka/2012/29_12s.pdf.

(in the case of Internet, email or Voice over IP (VoIP) communications) or for a period of 12 months (in case of other communications). Data about unsuccessful calls was also stored for the same periods. Moreover, the legal framework regulating the access to data retention data was completely arbitrary and considerably less stringent than comparable provisions on wire-tapping."[192] According to the European Information Society Institute, "*the introduction of these obligations constituted a substantial encroachment upon the private life of individuals – especially because this mandated blanket monitoring of all inhabitants of Slovakia, regardless of their innocence or prior behaviour. The data retention requirements mandated that every day the data about every inhabitant of Slovakia must be collected, amassing a profile of who called whom, to whom someone sent an SMS or email, when the person sent it, from which location, using what type of device or service, how long the communication took, and many others details. It almost goes without saying that combining all this information made it possible to perfectly analyse the movements of every inhabitant of Slovakia using a mobile phone or the internet.*" The Constitutional Court applied here the proportionality between the protection of privacy of individuals and state interests in criminal investigations.

8.2.3 Consequences for the interception of telecommunication

Slovak authorities may safeguard and surrender computer data for criminal proceeding purposes. Intrusive measures as well as protective instruments are primarily focused on real-time communications and specifically on telecommunications. On the other hand, the Slovak criminal law already has experience with stored data (communication). Recently, a new provision in the Code of Criminal Procedure states:[193]

> *"Section 90*
>
> *Safeguarding and surrendering computer data*
>
> *(1) If the clarification of facts relevant to criminal proceedings requires access to safeguard stored computer data, including operational data saved through the computer system, the presiding judge of a panel or a prosecutor prior to the commencement of criminal prosecution or in pre-trial proceedings, respectively, may issue an order based on circumstantial reasons to the person who has possession of or control over such data, or to the provider of such services, requesting them to*

192 EDRI.prg. Slovakia: Mass surveillance of citizens is unconstitutional. Online: https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/.

193 Ibid. The Code of Criminal Procedure.

a) safeguard and maintain integrity of such data,

b) enable making and keeping copies of such data,

c) prevent access to such data,

d) remove such data from the computer system,

e) surrender such data for the purposes of criminal proceedings.

(2) The order referred to in paragraph 1 shall have to specify the period during which the data are to be safeguarded, not exceeding 90 days; a new order shall have to be issued for any extension of that period.

(3) Where there is no longer a need to safeguard computer data, including operational data for the purposes of criminal proceedings, the presiding judge of a panel or a prosecutor prior to the commencement of criminal prosecution or in pre-trial proceedings, respectively, shall issue an order reversing the obligation to safeguard the data.

(4) The order referred to in paragraphs 1 to 3 shall be served on the person who has possession of or control over such data, or on the provider of such services, who may be also imposed the duty to treat the measures set out in the order as confidential.

(5) The person who has possession of or control over computer data shall surrender these data, or the provider of services shall surrender the information that is in his possession or under his control in connection therewith to the authority that issued the order pursuant to paragraph 1."

Also, an example is the old provision implemented for the retention of traffic data in the Act No.351/2011 Zb. on electronic communications. The Slovak Constitutional Court has repealed this provision (paragraphs 5, 6, 7 and 8) as unlawful regarding the European trends in mass surveillance issues: [194]

"Section 58

(1) User identification means a unique identification code, login name, or other unique mark assigned to a subscriber at the conclusion of the contract of the provision of public services or to a user during a registration of the Internet access services or communications services via Internet.

(2) Cell identification (cell ID) means the identity of the radio mobile network cell from which a call via a mobile terminal equipment originated or terminated.

(3) For the purposes of retaining data under Subsections 5 to 8, telephone service means the calls including telephone calls, voice mail, conference calls and data

194 Ibid. The Code of Criminal Procedure.

transmission, supplementary services including call forwarding and call transfer and messaging and multimedia services including SMS, enhanced media services (EMS) and MMS.

(4) For the purposes of retaining data under Subsections 6 and 7, unsuccessful call attempt means the call which has been successfully connected to the calling party terminal equipment but such a call has not been answered by the called user or his terminal equipment or there has been a network management intervention.

(5) For the purposes under Subsection 7, the undertaking shall be obliged to retain traffic data, location data and data of the parties who communicated from the date of making the communication during:

a) Six months in case of Internet access, Internet electronic mail and telephoning through Internet, and

b) Twelve months in case of other types of communication.

(6) The undertaking shall retain data under Subsection 5 in the scope in which it produces or processes while provisioning a service or network. The undertaking shall retain the data under Subsection 5 related to the unsuccessful call attempts which the undertaking produces or processes and retain in terms of the telephone numbers, or records in case of the Internet data. The data related to unconnected calls shall not be retained. The list of data which the undertaking shall be obliged to retain under this Subsection and Subsection 5 is referred to in Annex2.

(7) On the basis of a written request and without delay, the undertaking shall be obliged to provide data retained under Subsections 5 and 6 including the subscriber's data in the scope under Section 63, Subsection 1, Letter b) under conditions set in Section 63, Subsection 6 to the bodies acting in the criminal proceedings, court and other state body for the purposes of investigation, detection and prosecution of criminal offences related to terrorism, illegal trading, organized criminal activity, leakage and threatening of the concealed facts and to criminal offences committed by dangerous grouping; the data and information shall be retained only in an electronic form.

(8) The undertaking shall be obliged to administer a yearly statistic on the retained data which shall contain:

a) A number of cases in which the required data was provided to other state bodies under Section 55, Subsection 6,

b) The time elapsed between the date on which the data were retained and the date on which an authority acting in a criminal proceeding, court or other state body requested the provision of the data, and

c) The number of cases where the requests for data could not be met.

(9) Statistics under Subsection 8 shall not contain personal data. The undertaking shall provide statistics under Subsection 8 to the Ministry within January, 31 of the next year. The Ministry shall subsequently submit statistics to the European commission.

(10) Where retaining the data under Subsection 6, the undertaking shall ensure that:

a) The retained data shall be of the same quality and subject to the same security and protection as the data which the undertaking processes or retains when providing networks or services,

b) The data shall be subject to the relevant technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, unauthorised or unlawful storage, processing, access or publishing,

c) The data shall be subject to the relevant technical and organisational measures to ensure that the data can be accessed by the authorised persons only acting under the authority or power of attorney of the undertaking and authorities acting in a criminal proceeding, court or other state bodies and their entrusted or otherwise authorised members or staff,

d) The data, except those that have been provided and secured, shall be destroyed at the end of the period of retention."

Also, protection of the confidentiality and integrity of information systems is a specific part of the Slovak law of electronic communications. The respective provisions of the Electronic Communications Act read as follows:[195]

"Section 64

Security and Integrity of Public Networks and Services Section

(1) The undertaking that provides public networks or public services shall be obliged to take appropriate technical and organisational measures to protect security of its networks and services, which with regard to the technology state shall ensure such a level of security that is adequate to the risk posed. Measures shall be taken in particular to prevent and minimise the impact of security incidents on users and interconnected networks.

195 Act No.351/2011 Zb. On Electronic Communication. Unofficial translation. Online: http://www.teleoff.gov.sk/data/files/22211.pdf.

(2) The undertaking that provides public networks shall be obliged to maintain the integrity of its networks in order to ensure the continuity of provisioning services over those networks.

(3) The undertaking that provides public networks or services shall be obliged, without delay, to inform the Office about a breach of security or integrity that has had a significant impact on the operation of networks or services.

(4) If it is in the public interest, the Office shall publish information under Subsection 3 or, on the basis of a request of the Office, the undertaking shall publish such information.

(5) In the case of a particular risk of a breach of the network security, the provider of public services shall be obliged to inform subscribers concerned about such a risk and any possible remedies, including likely costs necessary to avert the threat.

(6) The undertaking that provides public networks or services shall be obliged:

a) Upon the request of the Office, to provide the relevant information necessary to assess security and integrity of its services and networks, including the documented security policies,

b) To enable a security audit carried out by a qualified independent person selected by the Office or the Office itself, while the cost of the audit shall be covered by the undertaking.

c) To provide the results of the audit to the Office and, upon the request, the Office for protection of personal data,

d) To cooperate with the Office in investigation of cases of non-compliance with regulations and their impact on network security and integrity and, upon the request, to provide the Office with relating relevant information.

(7) The details on maintaining the network integrity and parameters thereof and the notification obligation of the undertaking under Subsections 3 to 5 and 6, Letter a) shall be regulated by a generally binding legal regulation issued by the Office.

(8) The undertaking providing public networks and associated facilities shall be obliged to ensure that its network and associated facilities comply with technical standards and technical specifications for networks or services under Section 14, Subsection 2, Letter q) in terms of:

a) Network traffic security,

b) Network integrity maintaining,

c) Service interoperability,

d) Terminal equipment connection.

(9) Where appropriate, the Office shall provide information under Subsection 3 to regulatory authorities in the Member States and agency ENISA. The Office shall annually submit the European Commission and ENISA a summary report on the notifications under Subsection 3 and any related measures taken."

Furthermore, the protection of confidentiality and the integrity of information systems and information networks is the main subject of Cyber security law, which is currently in the progress.[196] Protection of the core area of privacy is defined also *stricto sensu* by the Civil Code from 1964. This old legislation doesn't reflect the recent problematic nature of the concept of privacy or its current technology determination. It includes only very general provisions whose meanings for everyday life in an information society are highly uncertain.

8.2.4 Statutory protection of personal data

In the age of Slovak independence, the protection of personal data became important as a reflection of constitutional citizens' privacy protection. The Slovak Penal Code (Act No.300/2005 Zb.) covers criminal liability for the unlawful infringement of telecommunication (e.g., information/data breach). Likewise, The Slovak Republic is a member of the Budapest treaty,[197] so these provisions reflect standard types of crimes laid down therein. Typical crimes are breach of mailing secrets; harm done to and abuse of an information carrier; and breach of confidentiality of spoken utterance and other personal expression.

The most important crimes related to the personal data are:[198]

"Section 196

Breach of Mailing Secrets

196 NASES. Cyber Security Concept of the Slovak Republic. Online: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1.

197 Budapest Convention on Cybercrime. Online: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=02/06/2010&CL=ENG.

198 Act. No. 300/2005 Zb. Penal Code. Unofficial translation: Ďurčová, M. Online: www.legislationline.org/documents/id/16895 and System ASPI, ASPI Translation. Wolters Kluwer. 2016 300/2005 Z.z. Trestný zákon (Penal Code). [Sections 247, 247a, 247 b, 247c, 247d] Online: http://www.aspi.cz.

(1) Any person who intentionally breaches the secrecy of letter through spying or opening a sealed letter or other written communication delivered by postal service or in other habitual manner, shall be liable to a term of imprisonment of up to three years.

(2) Any employee of the provider of postal service or electronic communication service who commits the offence referred to in paragraph 1, or wilfully enables another to commit such offence, or who alters or withholds a written communication delivered by postal service or in other habitual manner or communication transferred via electronic communication service shall be liable to a term of imprisonment of one to five years.

(3) The offender shall be liable to a term of imprisonment of four to ten years if he commits the offence referred to in paragraphs 1 or 2,

a) and causes substantial damage through its commission,

b) by reason of specific motivation,

c) acting in a more serious manner.

Section 247

Illegal Access to a Computer System

(1) Whoever overcomes security measures, thus obtaining illegal access to a computer system or part thereof, shall be punished by a prison sentence of up to two years.

(2) A prison sentence of one to five years shall be imposed upon an offender if they committed an act referred to in Subsection 1 and thus cause significant damage.

(3) A prison sentence of three to eight years shall be imposed upon an offender if they committed an act referred to in Subsection 1

a) and thus cause damage of a large extent, or b) as a member of a dangerous group.

Section 247a

Illegal Intervention into a Computer System

(1) Whoever restricts or interrupts the functioning of a computer system or part thereof by a) illegally entering, transmitting, damaging, deleting, reducing the quality of, altering or suppressing computer data or making them inaccessible, or b) illegally intervening into the hardware or software of a computer and destroying, damaging, deleting, altering the obtained information or reducing the quality of the obtained information, shall be punished by a prison sentence of six months to three years.

(2) A prison sentence of three to eight years shall be imposed upon an offender if they committed an act referred to in Subsection 1

a) and thus cause significant damage,

b) and thus cause serious failure in the activities of a state authority, local government authority, court or other public authority,

c) by misusing the personal data of another person in order to gain the trust of a third party.

(3) An offender shall be punished by a prison sentence of four to ten years if they committed an act referred to in Subsection 1

a) and thus cause damage of a large extent,

b) and thus cause serious failure in critical infrastructure, or c) as a member of a dangerous group.

Section 247 b

Illegal Intervention into Computer Data

(1) Whoever intentionally damages, deletes, alters, suppresses or makes computer data inaccessible or reduces their quality in a computer system or part thereof, shall be punished by a prison sentence of six months to three years.

(2) A prison sentence of three to eight years shall be imposed upon an offender if they committed an act referred to in Subsection 1

a) and thus cause significant damage,

b) and thus cause serious failure in the activities of a state authority, local government authority, court or other public authority,

c) by misusing the personal data of another person in order to gain the trust of a third party.

(3) An offender shall be punished by a prison sentence of four to ten years if they committed an act referred to in Subsection 1

a) and thus cause damage of a large extent,

b) and thus cause serious failure in critical infrastructure, or c) as a member of a dangerous group.

Section 247c

Illegal Capture of Computer Data

(1) Whoever illegally captures computer data through technical means of non-public transmissions of computer data to or from or within a computer system, including electromagnetic emissions from a computer system that contains such computer data, shall be punished by a prison sentence of six months to three years.

(2) Whoever as an employee of a provider of an electronic communications service commits the act referred to in Subsection 1 or intentionally facilitates the commission of such act by another person, or alters or suppresses a message submitted through an electronic communications service, shall be punished by a prison sentence of one to five years.

(3) A prison sentence of three to eight years shall be imposed upon an offender if they committed an act referred to in Subsection 1 or 2

a) out of a special motive,

b) in a more serious manner of conduct, or c) and thus cause significant damage.

(4) A prison sentence of four to ten years shall be imposed upon an offender if they committed an act referred to in Subsection 1 or 2

a) and thus cause damage of a large extent, or

b) as a member of a dangerous group.

Section 247d

Production and Possession of Access Devices, Passwords to Computer Systems or other Data

(1) Whoever, with the intention of committing the criminal offence of illegal access to a computer system under Section 247, illegal intervention into a computer system under Section 247a, illegal intervention into computer data under Section 247 b or illegal capture of computer data under Section 247c, produces, imports, procures, buys, sells, exchanges, puts into circulation or howsoever provides access to a) a device, including a computer programme, created for illegally accessing a computer system or part thereof, or b) a computer password, access code or similar data enabling access to a computer system or part thereof, shall be punished by a prison sentence of up to two years.

(2) A prison sentence of six months to three years shall be imposed upon an offender if they committed an act referred to in Subsection 1 and thus cause significant damage.

(3) A prison sentence of one to five years shall be imposed upon an offender if they committed an act referred to in Subsection 1

a) and thus cause damage of a large extent, or

b) as a member of a dangerous group.

Section 377

Breach of Confidentiality of Spoken Utterance and Other Personal Expression

(1) Any person who breaches the confidentiality of private spoken utterance or other personal expression by its unlawful recording, and makes such recording accessible to a third person or uses it otherwise, and thus causes serious prejudice to the rights of another, shall be liable to a term of imprisonment of up to two years.

(2) The offender shall be liable to a term of imprisonment of between six months and three years if he commits the offence referred to in paragraph 1

a) as a member of an organised group,

b) and causes substantial damage through the commission of such offence, or

c) with the intention of obtaining substantial benefit for himself or another.

(3) The offender shall be liable to a term of imprisonment of between six months and five years if he

a) commits the offence referred to in paragraph 1 as a public official,

b) and causes large-scale damage through the commission of such offence, or

c) commits such offence with the intention of obtaining large-scale benefit for himself or another."

Protection of professional secrets in criminal procedural law is guaranteed by dual concepts: the obligation to maintain confidentiality (in Anglo-American law as an attorney-client privilege) and the ban on witness examination. For example, Act No. 586/2003 Zb. on the Legal Profession,[199] which rules the attorney profession, in Section 23 of this act the scope of the obligation to maintain confidentiality is defined:[200]

"Section 23

(1) The lawyer is obliged not to reveal any information learnt in connection with the practice of law and shall treat such information as strictly confidential.

(2) The lawyer may be released from the duty of confidentiality by the client, and after his client's death or dissolution only by the client's legal successor. If the client has several legal successors, release from the duty of confidentiality shall take effect subject to the prior written consent of all legal successors.

199 Act No. 586/2003 Zb. on the Legal Profession and on Amending Act No. 455/1991 Zb. on the Business and Self-Employment Services (Business Licensing Act) as amended. Unofficial translation. Online: http://www.ccbe.org/fileadmin/user_upload/NTCdocument/en_slovak_rep_parlia1_1188889665.pdf.

200 Act No. 586/2003 Zb. on the Legal Profession (unofficial translation by CCBE.eu). Online: http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_transposition_slo1_1202123946.pdf.

(3) The lawyer shall not disclose confidential information despite his having been released from this duty by the client or all his legal successors, if the lawyer comes to a conclusion that any such release and disclosure would be detrimental to the client and might cause harm to the client.

(4) The lawyer may reveal information to a person, to whom he wishes to issue a derivative power of attorney in respect of individual legal acts, provided that such a person himself is bound by confidentiality under separate legal rules.

(5) The lawyer may disclose any confidential information to the court of law or any other authority, if the matter handled by such authorities concerns a dispute between the lawyer and his client, or the client's legal successor.

(6) The lawyer may not claim confidentiality in a disciplinary proceeding under this Act. Details shall be laid down in the Bar's Disciplinary Rules.

(7) The duty of confidentiality shall be observed during temporary suspension from the practice and shall even survive the lawyer's disbarment.

(8) The duty of confidentiality shall apply mutatis mutandis to:

a) employees of the lawyer, of the general non-commercial partnership, of the limited liability partnership, or of a limited liability company,

b) other persons, who are in connection therewith engaged in the provision of legal services,

c) members of the Bar's governing bodies and its employees [Sec. 66(4)].

(9) The duty of confidentiality shall not apply to any cases of lawful disclosure that would prevent a crime.

(10) The duty of confidentiality under a separate legal rule1 shall not be affected or prejudiced hereby."

On another hand, the Code of Criminal Procedure brings a ban on witness examination in the case of an attorney admitted to the bar. Witnesses shouldn't be asked to testify on matters that involve secret data, the data they are obliged to keep secret, except when the competent body waives the confidentiality obligation. The waiver can be denied only in the case of danger to the defence or the security of the State, or if the examination could cause other equally serious damage. The denial of a waiver made by an authority must be always justified. Witness can't be asked to testify if his testimony would constitute a breach of the confidentiality obligation

prescribed or recognised by law or by an international treaty, unless that obligation is waived by the competent body or the body in whose interest such obligation was imposed.

This ban on interrogation doesn't apply to the testimony given in respect of an offence that the witness has an obligation to report under the Criminal Code.

Also, the principle of purposeful limitation of personal data is incorporated in Personal Data Protection Act (Act No. 122/2013 Zb.). The most important provisions lay down the purpose of limitation next to the General Data Protection Regulation (Regulation (EU) 2016/679).[201]

8.3 Powers for Accessing Telecommunication Data

8.3.1 Overview

The Code of Criminal Procedure in the Slovak Republic is the central point for the law enforcement authorities to intercept electronic communication and to otherwise access electronic communications data for the purpose of criminal investigations. As was mentioned before, the most important are provisions regulating: General duty to surrender a thing (Section 89), Safeguarding and surrendering computer data (Section 90), Interception (Section 115) and the recently repealed provision on Access to traffic and location data (Section 116).

Strong powers for the law enforcement authorities accessing telecommunication data can be found in the Act on the Protection against Interception, which stipulates the conditions required for the use of ITM (intelligence technical measures) without the prior consent of the person whose privacy is infringed upon by the state body which uses the ITM.

201 Act No. 122/2013 Zb. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Zb. (Unofficial translation) Online: http://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf.

8.3.2 Requirement of (reasonable) clarity for powers in the law of criminal procedure

The situation about requirements of (reasonable) clarity for powers in the law of criminal procedure is very close to Czech law. The fundamental rules that govern Slovak criminal procedural law are provided in Section 2 of the Code of Criminal Procedure. The Fundamental Rules of Criminal Procedure are based on the principle that no person may be prosecuted as accused on other than the legal grounds and in another manner than that provided for under the present Act. Another very important principle reads that fundamental rights and freedoms of persons may be, in cases permitted by law, interfered with to the extent necessary to achieve the purpose of criminal proceedings with due respect for the dignity of persons and their privacy. Any interference with fundamental rights and freedoms under the Code of Criminal Procedure before the commencement of the criminal prosecution or in pre-trial proceedings shall be decided by a judge for pre-trial proceedings; the judge for pre-trial proceedings shall also decide on other matters as provided for by the Code of Criminal Procedure. One of the basic principles of criminal procedure rules is that any person subject to criminal prosecution shall be presumed innocent until proven guilty by a final sentencing judgment.

Other fundamental criminal procedure principles are:[202]

- A prosecutor represents the State in criminal proceedings. Unless the Code of Criminal Procedure, an international treaty promulgated in a manner prescribed by law (hereinafter referred to as "international treaty") or the decision of an international organisation which is binding on the Slovak Republic provides otherwise, the prosecutor shall have the duty to prosecute all criminal offences that came to his knowledge.
- Unless the Code of Criminal Procedure provides otherwise, the bodies involved in criminal proceedings and the courts shall act ex officio. They shall have the duty to deal with cases involving detention as a matter of priority and without undue delay. The authorities

202 Section 2 of 301/2005 Zb. Code of Criminal Procedure. The European e-Justice Portal. Unofficial translation.

involved in criminal proceedings or the courts shall not take account of the petitions whose content infringes on the fulfilment of this duty.

- Every person shall have the right to a fair hearing of his criminal case by an independent and impartial tribunal in a reasonable time and in his presence, and to have an opportunity to comment on any adduced evidence, unless the Code of Criminal Procedure provides otherwise.
- No person may be prosecuted in respect of an act for which he had already been finally convicted or from which he had been acquitted. This principle shall not exclude the use of extraordinary remedies as prescribed by law.
- Every person subject to criminal prosecution shall have the right to defence.
- The authorities involved in criminal proceedings shall proceed so as to properly establish the facts of the case that do not give rise to reasonable doubts, to the extent necessary for making the decision. They shall procure the evidence as part of their official duties. The parties shall also be granted the right to procure the evidence. The authorities involved in criminal proceedings shall thoroughly clarify the circumstances regardless of whether they prejudice or benefit the accused, and they shall take the evidence in either direction so as to enable the court to arrive at a fair decision.
- The court may also take other evidence than those proposed by the parties. The parties shall have the right to supply the evidence proposed by them.
- The authorities involved in criminal proceedings and the court shall evaluate the legally obtained evidence in accordance with their deep conviction based on the careful examination of all the facts of the case, separately and jointly, irrespective of whether they were supplied by the court, the authorities involved in criminal proceedings or by one of the parties to the proceedings.
- All the authorities involved in criminal proceedings shall co-operate with associations of citizens and shall make use of the educational impact thereof.
- All parties shall have equal status before the court.

- Criminal prosecution before the court shall only be initiated on the basis of a motion or an indictment filed by a prosecutor who shall represent the prosecution or the motion in the proceedings before the court.
- In criminal proceedings before the court, the decision shall be made by a panel of judges, a single judge or by a judge for pre-trial proceedings. A presiding judge of a panel, a single judge or a judge for pre-trial proceedings shall have the sole authority to decide the case only when the law expressly provides for it.
- Criminal cases shall be heard in open court. Public attendance may be excluded from the main hearing or open court hearing only in cases explicitly provided for under the Code of Criminal Procedure. The judgment shall always be announced in open court.
- Proceedings before the court shall be oral; exceptions are provided for under this Act. The examination of evidence shall be carried out by the court, which, however, leaves the examination of the accused, witnesses and expert witnesses to the parties, starting with the one that proposed or procured the evidence.
- When deciding at the main trial, open or closed court hearing, the court may only take account of the evidence taken during the hearing, unless otherwise provided by law.
- If the accused, his legal guardian, the injured party, a participating person or witness declares that he does not speak the language of the proceedings, he shall have the right to be assigned an interpreter or a translator.

Also, in many criminal cases the Supreme Court of the Slovak Republic or the Slovak Constitutional Court has interpreted these fundamental rules to define reasonable clarity for powers in the law of criminal procedure.

8.3.3 Differentiation and classification of powers in the law of criminal procedure

Coercive powers related to telecommunications data are, in Slovak criminal procedure, defined by criminal law legislation, which regulates wiretapping on one side and retention of traffic data on the other side. Duties and procedures that apply on the side of providers of electronic communications services are defined in the Electronic Communications Act, while

procedures that apply on the side of the Police or Prosecution Service are laid down in the Code of Criminal Procedure or Act on the Protection against Interception (see the Chapter I.A.1).

The reason for such separation is primarily the fact that wiretapping and data retention serve other purposes than just criminal procedure. Consequently, provisions laid down in the Electronic Communications Act cover, in general, the obligations of providers of services of electronic communications. Also, they specify only purposes for which respective data might be requested. Finally, it is important to note that the situation here is currently unclear due to the Constitutional Court decision about the invalidity of relevant provisions in the Electronic Communications Act.

8.4 Interception of Content Data

8.4.1 Object of interception, special protection of confidential communication content and execution of telecommunication interception

Slovak law broadly defines the object of an interception. The procedural concept of execution is based on the order or approval to intercept and record telecommunications. Another important term is ITM (intelligence-technical measures/means). These measures are defined as electro-technical, radio- technical, photo-technical, optical, mechanical, chemical, and other technical measures and equipment or their sets, used in a covert manner in: a) searching for, opening, examination, and assessment of mail and other transported packages; b) monitoring and recording of telecommunication activities; c) making and using the visual, audio, and other recordings.

Regarding access to on-going telecommunication, the abovementioned provisions cover this type of interception. The investigator may intercept any data that are "in traffic" – from the moment it is sent from the source device to the moment it is received by the destination device. The provisions on safeguarding and surrendering computer data pursuant to Section 90 of the Code of Criminal Procedure regulate access after the end of telecommunication transmission (see above).

Pursuant to the Section 115 of the Code of Criminal Procedure, if the accused is found to be in communication with his defence counsel, no information thus obtained may be used for the purposes of criminal proceedings, and any such information must be forthwith destroyed in a prescribed manner. This regulation will not apply to information relating to a case in which a lawyer does not represent the accused as his defence counsel. A similar situation applies for the duty to surrender a thing pursuant to Section 89 Paragraph 2, respectively for the safeguarding and surrendering of computer data pursuant to the Section 90 of the Code of Criminal Procedure.

The Code of Criminal Procedure doesn't stipulate which modes of interception law enforcement authorities should use. Minor regulations regarding ITM are embodied in the Act on the Protection against Interception (see above). Also, these activities are conducted by the Slovak Police Corps pursuant to the Section 36 of the Act No. 171/1993 Zb. on Police Corps.

8.4.2 Duties of telecommunication service providers to cooperate

Possible addressees of duties of cooperation are any subjects able to assist in criminal procedure. Therefore, any natural or legal person is required to comply with letters of request from law enforcement authorities for the performance of their actions without undue delay. The related provision is in Section 3 of the Code of Criminal Procedure. Public authorities (e.g., self-governing higher territorial units, municipalities and other legal entities and natural persons) have the duty to provide assistance to the courts and authorities involved in criminal proceedings in the fulfilment of their tasks in relation to criminal proceedings.

The content of duties to cooperate arises from the essence of criminal procedure. According to Section 63 of the Act on electronic communications, the subject of telecommunications secrecy shall cooperate with public authorities. This is also valid for provision of the technical infrastructure; security requirements for data transfers by communication service providers; checks, filtering, and decryption obligations of communication service providers. The subject of telecommunications secrecy is usually the content of conveyed messages, related data of the communicating parties which are the telephone number, business name and the place of business of a legal

person, or business name and the place of business of a natural person – undertaker or the personal data of a natural person which are the name, surname, title and permanent residence address (e.g., the data published in the telephone directory shall not be subject to telecommunications secrecy), traffic data, and location data. Everybody who becomes familiar with the subject of telecommunications secrecy when providing networks and services, using the services, accidentally or otherwise, is obliged to keep telecommunications secrecy.

8.4.3 Prerequisites of interception orders

The competent authority to warrant the interception and recording in a criminal procedure is always a legitimate body (judge or prosecutor). Usually, the order to intercept and record telecommunications is issued by the presiding judge of a panel prior to the commencement of criminal prosecution, or by a judge for pre-trial proceedings following a motion from a prosecutor. If the matter bears no delay and a prior order from a judge for pre-trial proceedings cannot be obtained, the order may be issued by a prosecutor before the commencement of criminal prosecution or in pre-trial proceedings, unless the interception and recording of telecommunications involves entry into the dwelling of a person. A judge for pre-trial proceedings must confirm this type of order within 24 hours of its issuance. Failing that, the order becomes null and void and the information obtained on its basis may not be used for the purposes of criminal proceedings and has to be immediately destroyed in a prescribed manner.

The order to intercept and record telecommunications has to be in writing and based on circumstantial reasons, separately for each telephone subscriber or other technical equipment. The order has to specify the telephone subscriber or technical equipment and, if known, the person whose telecommunications are intercepted and recorded, and the length of time during which the interception and recording of telecommunications are to be performed.

On another hand, the request to grant approval to use ITM according to the Act on protection against interception must be submitted in writing as well, and must contain the following data:

a) specification of the type of ITM to be used and the location of its use, the proposed duration of its use, data on the person against whom the use of this technical-intelligence measure is directed,
b) information on the previous ineffectual, or considerably difficult, disclosure and documentation of activities, which constitute the reason for submitting the request,
c) the rationale for using ITM.

As we demonstrated, the substantive prerequisites of interception orders according to the Code of Criminal Procedure are very similar to the Czech Code of Criminal Procedure.

To intercept and record telecommunications is possible only where criminal proceedings are conducted in investigation of a felony, corruption, a criminal offence of the abuse of power of a public official, a criminal offence of laundering the proceeds of crime, or in respect of an intentional criminal offence where so provided by a promulgated international treaty. Also, there must always be reasonable grounds to believe that interception will reveal facts that are materially relevant for criminal proceedings. In criminal proceedings conducted in respect of an intentional criminal offence which is different from the one referred to in the above mentioned list, the order to intercept and record telecommunications may be issued by the presiding judge of a panel or, prior to the commencement of prosecution or in pre-trial proceedings, by a judge for pre-trial proceedings acting on a motion from a prosecutor, but only with the consent of the subscriber to the telecommunication equipment subjected to interception or recording.

On the other hand, substantive prerequisites for interception orders according to the Act on protection against interception are entirely vague. Even this law does not apply to the criminal proceeding: it is very often used by investigators. Basically, this law entitles Police Corps, the Slovak Information Service, Military Intelligence, the Railway Police, the Corps of Prison and Judiciary Guards, and the Customs Board to shift obtained evidence from the intelligence regime to the criminal procedure. It is stated that ITM shall

be used only if it is required in a democratic society to safeguard the security and defence of the country, to prevent and reveal criminal activities, or to protect the rights and freedoms of other persons. By using ITM, the essential right or freedom can be infringed upon only to the required extent and for a period of time not longer than needed to attain the legal goal which it serves. The data obtained by ITM shall be used exclusively for achieving the objective when fulfilling the tasks of the state. Finally, ITM can be used only on the basis of prior written approval from a legitimate judge. In an exceptional case, if there is reasonable suspicion of a crime being committed and ITM might be used by the Police Corps to fulfil its tasks, if the case is to be dealt with immediately and the approval of a legitimate judge cannot be obtained in advance, the Police Corps may use ITM even without prior approval.

Regarding the time limit, the interception and recording, according to the Code of Criminal Procedure, may not exceed six months. This period may be extended by another two months, also repeatedly, on a motion from a prosecutor or a judge for pre-trial proceedings. Interception and recording, according to the Act on the Protection against Interception, may not exceed six months. This period may be extended by another 6 months, also repeatedly, on a motion from the Police Corps or another entitled authority.

According to the Code of Criminal Procedure, Police officers or a competent department of the Police Corps shall be obliged to continuously review the grounds for the order to intercept and record telecommunications. Where such grounds cease to exist, interception and recording of telecommunications shall have to be discontinued, even if this is before the expiry of the time limit. This fact shall be immediately notified in writing to the entity that issued the order to intercept and record telecommunications; in pre-trial proceedings, it shall also be notified to the prosecutor.

The legitimate judge who has granted approval to use ITM is required to systematically review the existing rationale of their use pursuant to the Act on the Protection against Interception. If the rationale no longer applies, he is obliged to issue a decree immediately that the use of these measures cease. However, in our opinion, the practices of authorities are very unclear in this matter and no relevant statistics have been published yet.

8.4.4 Duties to record, report, and destroy

According to the Code of Criminal Procedure, if the record of telecommunications is to be used as evidence, a verbatim transcript made by the officer of the Police Corps carrying out the interception of telecommunications has to be attached, wherever the recording makes it possible, containing information about the place, time and legal grounds for interception. A verbatim transcript of the record of telecommunications, which is not secret (e.g., classified information), signed by the Police Corps officer who drew it up, must be inserted in the file. In the situation where the verbatim transcript of telecommunication records contains a classified fact, it is classified according to separate legal provisions. Also, the transcript of telecommunications can be used as evidence after the interception of telecommunications has been discontinued. In pre-trial proceedings, where the circumstances of the case warrant it, the recording of telecommunications may be submitted to the court even without a transcript of the recording, if the accompanying report gives the data concerning the time, place and legality of interception, and concerning the person subject to the recording of telecommunications, provided that the recording of telecommunications is intelligible.

If the interception and recording did not produce any facts relevant to the criminal proceedings, the criminal procedure authority or the relevant department of the Police Corps have to destroy the obtained records forthwith in a prescribed manner. The protocol for the destruction of the recordings must be inserted in the file.

According to the Act on the protection against interception, if the information obtained by using ITM is to be used as the evidence in a criminal procedure, the state body must produce a written record with the data on the location, time, and legitimacy of using ITM. Also, he must enclose the recording and its verbatim transcription with the written record. Information obtained by using ITM, which does not apply to the rationale of their use cited in the request, can be used in the criminal procedure only if it concerns the criminal activity in connection with which ITM has been permitted to be used.

If ITM has been used in contravention to the law, no state body or another body of public power is allowed to use the recording obtained in such a way, or any other result of the illegal use of ITM as evidence, or to recognise it as evidence, except for a criminal or disciplinary procedure against the person who has made the recording illegally or has ordered it made. The recording or other result obtained illegally must be destroyed in the presence of a legitimate judge, authorised to grant the approval, within twenty-four hours of the illegal use of the ITM.

A written statement shall be produced on the destruction of the recording or of any other result, including the reason for destroying this recording or result, the personal data of the person who has ordered or approved the use of ITM (the title, name, surname, and position), the personal data of the person who has ordered or approved the destruction of the recording or of any other result (the title, name, surname, and position), and the personal data of the legitimate judge present during the destruction (the title, name, surname, position, and the identification of the competent court). Before being destroyed, the recording or any other result of the use of ITM must not be copied or transcribed in written or in any other form.

The destruction of the recordings is usually notified to persons who do not have the right to view the criminal file. This practice is unreported so far. The notification should be made by the body whose decision has finally settled the matter, or, in proceedings before the court, by the presiding judge of a panel of a first-instance court within three years from the date on which criminal prosecution in the case was finally concluded. However, this does not apply to proceedings concerning particularly serious felonies or felonies committed by organised groups, criminal groups or terrorist groups, or criminal offences committed by more than one person if at least one of the perpetrators is still under prosecution, or if the provision of such information could obstruct the purpose of criminal proceedings.

8.5 Collection and use of traffic data and subscriber data

The questionable and cancelled EU Data Retention Directive was fully implemented at the national level in the Code of Criminal Procedure and other

relevant laws. The collection and use of traffic data and subscriber data could be acquired by warrant pursuant to Section 115 (with higher requirements) of the Code of Criminal Procedure. Recently, the Slovak Constitutional Court has repealed the warrant according to Section 116 (with lower formal requirements) to disclosure and provision of telecommunications data. It looked at blanket data retention that does not distinguish between persons who can be connected to major criminal activity and other persons, does not conform to the rights to privacy and protection of personal data. Therefore, the court ruled that the mass surveillance of citizens (easy access to the data retention) is unconstitutional. The decision has been made in the context of proceedings initiated by Members of the Parliament in cooperation with the European Information Society Institute, a Slovakia-based think-tank EISi.[203] The Grand Chamber of the Constitutional Court in the matter No. PL. ÚS 10/2014 ruled that provisions of the Act on Electronic Communications, which until now required providers to retain the communication of their users, as well as provisions of the Penal Code, and the Police Force Act, which allowed access to this data, to be in contradiction to the constitutionally guaranteed rights of citizens to privacy and personal data. It does not comply with this constitutional order and international human rights instruments because it constitutes an inadequate intervention into the privacy of persons. As an effect, these provisions have been repealed. The Grand Chamber of the Constitutional Court after the proportionality test (see 8. 2. 2) ruled referring to EU Charter as follows:[204]

> *"Stemming from the statement of members of Parliament there appeared a question of conformity of provisions of law No. 351/2011 Zb. on electronic communications in relation to articles 7, art. 8 and art. 11 of the Charter which is legally binding for Member states in case when they exercise European Union law (art. 51 par.1 of the Charter). Disputed provisions of law on electronic communications are without any doubt a transposition of related regulation pertaining to the European Union law (Directive of European Parliament and*

203 Husovec, M., Lukic, M. *The quest for privacy in Slovakia: The case of data retention*. 2014. Online: https://www.giswatch.org/sites/default/files/the_quest_for_privacy_in_slovakia.pdf.

204 EU Agency for Fundamental Rights. Slovakia / Constitutional Court of the Slovak Republic / PL. ÚS 10/2014. Translation of the Court's decision. Online: http://fra.europa.eu/en/caselaw-reference/slovakia-constitutional-court-slovak-republic-pl-s-102014.

Council 2002/58/CE from 12 July 2002), related to processing of personal data and protection of private life in area of electronic communications [Directive on privacy and electronic communications (Ú. v. CE L 201, p. 37; Special edition 13/029, p. 514) and Directive of European Parliament and Council 2006/24/CE from 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Ú. v. EU L 105, p. 54)], and thus Charter in fully applicable even in this case on conformity of legal provisions."

When it comes to subscriber data, the Slovak Republic applies the same rules as the Czech Republic regarding Act No. 351/2011 Zb. on electronic communications. In the case of a call from a mobile telephone network where the calling party number is not available, providers usually track the presentation of the international mobile equipment identification – a unique identification of mobile terminal equipment functioning as a controlling technical measure to identify the goods (IMEI).

8.6 Access to (temporarily) stored communication data

For accessing permanently or temporarily stored data, the law enforcement authorities in the Slovak Republic usually use a measure called safeguarding and surrendering computer data pursuant to the Section 90 of the Code of Criminal Procedure (see above). If the clarification of facts relevant to criminal proceedings requires the safeguarding of stored computer data, including operational data saved through the computer system, the presiding judge of a panel or a prosecutor prior to the commencement of criminal prosecution or in pre-trial proceedings, respectively, may issue an order based on circumstantial reasons to the person who has possession of or control over such data, or to the provider of such services, requesting them to:

a) safeguard and maintain the integrity of such data,
b) enable making and keeping copies of such data,
c) prevent access to such data,
d) remove such data from the computer system,
e) surrender such data for the purposes of criminal proceedings.

As was mentioned before, to access permanently or temporarily stored data, the law enforcement authorities in the Slovak Republic usually use a measure called safeguarding and surrendering computer data pursuant to Section 90 of the Code of Criminal Procedure (see above).

The order must specify the period during which the data are to be safeguarded, not exceeding 90 days. A new order must be issued for any extension of that period. When there is no longer a need to safeguard computer data, including operational data for the purposes of criminal proceedings, the presiding judge of a panel or a prosecutor prior to the commencement of criminal prosecution or in pre-trial proceedings, respectively, shall issue an order reversing the obligation to safeguard the data. The order is served on the person who has possession of or control over such data, or on the provider of such services, who may be also given the duty to treat the measures set out in the order as confidential. The person who has possession of or control over computer data must surrender these data, or the provider of services must surrender the information that is in their possession or under their control in connection therewith to the authority that issued the order.

Finally, with these measures investigators usually undertake the procedure to issue a warrant for house search pursuant to Section 100 of the Code of Criminal Procedure or a warrant for searching other premises or landed property pursuant to Section 101 of the Code of Criminal Procedure.

8.7 Use of electronic communication data in judicial proceedings

8.7.1 Use of electronic communication data in the law of criminal procedure

The Code of Criminal Procedure does not specifically regulate the regime of electronically intercepted communication data in criminal proceedings. Authorities must follow the regulations given by Section 115 of the Code of Criminal Procedure or Sections of the Act on the protection against interception. The most important part of any interception is the transcript, which has to fulfil all formal requirements. Usually, a verbatim transcript

made by the officer of the Police Corps is attached to the criminal file, and must contain information about the place, time and legal grounds for interception. According to recent opinions, any elimination of the defects in the protocol by police could be challenged as manipulation with the consistency of the lawful evidence. A content of the recording is also an essential requirement of the protocol related to the recording of telecommunications. The recording may be used as evidence in a different criminal matter from the one that is subject to interception and recording of telecommunications only if such other matter is also heard in simultaneous proceedings concerning a criminal offence referred to in Section 115 Paragraph 1 of the Code of Criminal Procedure (a felony, corruption, a criminal offence of the abuse of power of public official, a criminal offence of laundering the proceeds of crime, or in respect of an intentional criminal offence where so provided by a promulgated international treaty).

8.7.2 Inadmissibility of evidence as a consequence inappropriate collection

In the criminal procedure, the examination of evidence is carried out by the court, which, however, leaves the examination of the accused, witnesses and expert witnesses to the parties, starting with the one that proposed or procured the evidence.

As a piece of evidence may consist of anything that may contribute to proper clarification of the matter and was obtained as evidence under the Code of Criminal Procedure, or under a special law (Act on protection against interception or Act on Police Corps). This is an important aspect of "legality of evidence" and is incorporated as a basic principle of the evidence production procedure.

Evidence is categorized as: testimonies of witnesses or experts; reports and expert opinions; a review of the testimony taken at the scene; recognition; reconstruction; investigative experiments; a survey of objects and documents relevant to criminal proceedings; and any notifications or information obtained by use of ITM or operative activities.

The authorities involved in criminal proceedings process information so as to properly establish the facts of the case and avoid giving rise

to reasonable doubts, to the extent necessary for making the decision. They procure the evidence as part of their official duties. Also, the parties are granted the right to procure evidence. The authorities involved in criminal proceedings thoroughly clarify the circumstances, regardless of whether they prejudice or benefit the accused, and they take the evidence in either direction so as to enable the court to arrive at a fair decision. The crucial principle for the evaluation of evidence is that authorities evaluate the evidence in accordance with their deep conviction based on careful examination of all the facts of the case, separately and jointly, irrespective of whether they were supplied by the court, the authorities involved in criminal proceedings or by one of the parties in the proceedings.

It is very important that the authorities involved in criminal proceedings and the court evaluate only legally obtained evidence. This legal aspect emphasizes the admissibility of the evidence, which is embodied in Section 2 Paragraph 12 of the Code of Criminal Procedure. Therefore, we can also conclude that the inadmissibility of the evidence is deduced mainly by the interpretation of the above-mentioned principles of the evidence-producing process.

In general, interceptions which were acquired against the law are evaluated as absolutely inadmissible evidence. Transcripts of such recordings cannot be entered into the criminal file or read before the court. According to the opinion of some scholars, evidence obtained against the law is passing its inadmissibility and procedural invalidity on the further evidence, which is arising from the content of the first inadmissible evidence.[205]

Also, emphasis is put on the interception of a communication between an attorney (defence counsel) and client. Pursuant to Section 115 Paragraph 1 of the Code of Criminal Procedure, no information thus obtained may be used for the purposes of criminal proceedings, and any such information must be immediately destroyed in a prescribed manner. However, this does not apply to information relating to a case in which a lawyer does not represent the accused as his defence counsel (criminal attorney).

205 Viktoryova, J. Turek, L. Evidence Admissibility in Pre-trial Proceedings. *Notitiae ex Academia Bratislavensi Iurisprudentiae,* 2009, Vol. 3, No. 2, p.13.

The challenge is a "dual" legal regime of the interception. The interception should be used in criminal proceedings only when it was conducted on the basis of Section 115 of the Code of Criminal Procedure. An interception carried out under another legal act, e.g., under the Act on protection against interception, should be used only for the purposes which are defined by this act. The problem comes with such a legal definition which is not limited to operative techniques only. According to this Act, ITM can be used exclusively for achieving the security and defence of the country, to prevent and reveal criminal activities, or to protect the rights and freedoms of other persons. This is a quite open definition which covers criminal procedure and pre-trial matters as well. To finish this ambiguous definition, it is further required that by using ITM the essential right or freedom can be infringed upon only to the required extent and for a period of time not longer than required to attain the legal goal which it serves.

In one notable case, where an interception carried out under the Act on protection against the interception was used in criminal procedure, the Slovak Constitutional Court declared that:[206]

> *"[T]here cannot be any doubt that the approval or order [to intercept] must be justified in each case, whether issued under the Criminal Code or under the Law for protection against interception. This is because it is a serious intrusion to the fundamental rights of persons. Also, they have no possibility to appeal […] Therefore they are entitled to review the validity of an issued order subsequently. Such a review requires specific arguments explaining facts needed to interfere with the right to privacy. Without such a justification relying on specific facts there is no review. At first glance, it might seem that, due to the secret nature of interception, it would be intolerable and counterproductive to state in the reasoning specific facts justifying the granting of an order, as these could disturb their purposes. In fact, the opposite is true. Precisely because of the secret nature of the interception, nothing prevents the court from mentioning the reasons which led to the order being issued."*

206 Decision of the Slovak Constitutional Court No. I. ÚS 274/05-73. Translation of author. Online: http://portal.concourt.sk/.

8.7.3 Use of data outside the main proceedings

Uses of data/information outside the main proceedings in Slovak criminal procedure are based on these assumptions:

- Criminal proceedings are conducted in respect of a felony, corruption, a criminal offence of the abuse of power of public official, a criminal offence of laundering the proceeds of crime, or in respect of an intentional criminal offence where so provided by a promulgated international treaty, and if there are reasonable grounds to believe that it will reveal the facts that are materially relevant for criminal proceedings; and
- Another matter is also heard in simultaneous proceedings.

In practice, it is questionable what "simultaneous proceedings" means.

One opinion stream belongs to the interpretation that two proceedings have to be simultaneous at the moment the evidence is obtained(recording).[207] The second scholars' opinion holds the argument that the two proceedings have to be at simultaneous at the moment the evidence is executed (the moment of the producing the evidence).[208]

Finally, there is always the possibility to use the evidence in another procedure if there is consent of the user of the intercepted station or a concerned person.

Regarding the use of data from preventive investigations, please see the previous chapter on inadmissibility of evidence as a consequence of inappropriate collection, where a case was in which an interception carried out under the Act on protection against the interception was used in a criminal procedure. Under certain circumstances, this type of the evidence could be used in a criminal procedure. But it has to fulfil formal criteria laid down by the Code of Criminal Procedure.

Data from foreign jurisdictions are obtained in accordance with the Code of Criminal Procedure or a valid mutual legal assistance.

---

207 Opinion of the Attorney General of the Slovak Republic from 18. 4. 2011, Nu. IV/1GPt 145/12-7, cited in Tittlova, M. *Korupcia: Vybrané kriminologické a trestnoprávne aspekty*. Bratislava: Wolters Kluwer, 2015, p.209.

208 Decision of Supreme Court of the Slovak Republic from 21. 9. 2011, file number 3 To2/2011. Online: http://www.supcourt.gov.sk

Under Section 533 of the Code of Criminal Procedure, the general rule is that any request for legal assistance shall, in addition to a precise description of the required act of assistance, contain a description of the facts of the offence which is the basis of the request, the legal denomination of the offence together with a verbatim wording of the pertinent legal provisions, the personal data of the accused or, as the case may be, of the victim or the witnesses if their examination is requested, as well as further details required for the proper execution of the requested legal assistance. The request shall contain the exact specification of the requesting authority, its file number, the date of the request and it shall bear the signature of the responsible officer and the round seal of the requesting authority. The request and the supporting documents shall be accompanied by a translation into a foreign language done by an official translator if, in relation to the requested State, such translation is required.

Under Section 532 of the Code of Criminal Procedure, requests for legal assistance emanating from the Slovak pre-trial authorities shall be transmitted abroad through the General Prosecutor's Office. Requests for legal assistance emanating from the Slovak courts shall be transmitted abroad through the Ministry of Justice. Finally, diplomatic channels are another option for cooperation.

8.7.4 Challenging the probity of intercepted data

Challenging the probity of intercepted data in Slovak law is different from the Czech possibility to review the interception decision by the Supreme Court. The Code of Criminal Procedure doesn't recognize such a procedure.

In the situation where the interception did not produce any facts relevant for criminal proceedings, the criminal procedure authority or the relevant department of the Police Corps must destroy the obtained records immediately in a prescribed manner. There should be a protocol on the destruction as part of the criminal file. According to Section 115 Paragraph 8 of the Code of Criminal Procedure, the destruction of the recordings shall be notified to persons who do not have the right to view the criminal file. Furthermore, the notification shall be made by the body whose decision has finally settled the matter, or, in proceedings before the court,

by the presiding judge of a panel of a first-instance court within three years from the date on which the criminal prosecution in the case was finally concluded. It is important to note that this will not apply to the proceedings concerning particularly serious felonies or felonies committed by organized groups, criminal groups or terrorist groups, or criminal offences committed by more than one person if at least one of the perpetrators is still under prosecution, or if the provision of such information could obstruct the purpose of criminal proceedings.

Currently, there is on-going discussion about possible options to challenge such interception decisions. In one related decision the Slovak Constitutional Court has established that: [209]

> *"The appeal against the consent, nor command [to interception] is not permitted. The concerned person is not able to seek protection at the general court in connection with the fact that his conversation has been intercepted. The general court could not review the eligibility of the issuance of a final consent or order, and it is precisely because the consent or order is a valid and enforceable decision, by which is the court bound. […] The concerned person whose conversation has been intercepted can challenge the illegality of the interception and the consequent usefulness of the recorded conversation as evidence in criminal court proceedings. He can do so only by the simultaneous fulfilment of two conditions. A criminal case has to reach the trial stage and the concerned person has to be a party to the criminal proceedings, either as a charged person or as a person claiming damages. Also, it means the protection by the criminal court will not come up in a case which does not come before the criminal court, nor in a case, in which the concerned persons are not parties to criminal proceedings."*

The Constitutional Court stated that unless the complainant argues that the records were obtained illegally, he can still put forward this argument in the context of criminal proceedings, particularly before the competent court in his defence. He may request to review illegally obtained evidence which therefore should not be taken in court's consideration. It will be a matter of a court or other law enforcement agencies to consider such an argument and draw conclusions from it. But also, it means that the person whose telephone conversation was intercepted must be able to defend

209 Decision of the Slovak Constitutional Court No. I. ÚS 274/05. Unofficial translation. Online: http://portal.concourt.sk/.

against the very fact of interception. The Slovak Constitutional court has divided this procedural right into two parts: a claim to a right to privacy, and also a claim against the use of interception of communications as evidence in criminal proceedings. Regarding these facts, the Slovak Constitutional court declared that illegal interceptions have intruded on the claimant's rights and his freedoms (were invalid due to lack of reasoning). He has repealed the orders to intercept and also settled the matter of adequate financial satisfaction, which has to be paid by state.

Therefore, the conclusion for the options to challenge the probity of intercepted data in Slovak Republic can be found in barely accessible procedural tools:

- Constitutional complaint (Act. No. 38/1993 Z. z., on the organization of the Constitutional Court of the Slovak Republic, proceedings and the status of its judges), or
- Private action for the protection of personality (Act No. 40/1964 Sb. Civil Code).

BIBLIOGRAPHY

Academic and related sources

Alexy, R. Constitutional Rights, Balancing and Rationality, 2003, *Ratio Iuris*, Vol. 16, No. 2, pp. 131-140. ISSN 0952-1917.

Bobek, M., Molek, P., Šimíček, V. *Komunistické právo v Československu*, Brno: Masarykova univerzita, 2009, 1005 p. ISBN 978-80-210-4844-7.

Gera, M. Mass surveillance of citizens is unconstitutional. Protecting digital freedom. *EDRi.org*. May 4, 2015. Online: https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/.

Harašta, J., Myška M., Budoucnost data retention, *Trestněprávní revue*, 2015, Vol. 14, No. 10, pp. 238-241. ISSN 1213-5313.

Myška, M. *Právní aspekty uchovávání provozních a lokalizačních údajů*, Brno: Masarykova univerzita, 2013, 133 s. ISBN 978-80-210-6462-1.

Chudomelová, Z., Beran, M., Jadrný, V., Němečková, Š., Novák, J. *Zákon o elektronických komunikacích – komentář*, Praha: Wolters Kluwer, 2016, xxii, 507 p. ISBN 978-80-7552-100-2.

Kant, I. The Universal Principle of Right: The Laws of Freedom as Moral, Judicial and Ethical, *Illinois Law Review*, 1914-1915, Vol. 9, No. 3, p. 574. ISSN 0276-9948.

Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D. *Zákon o ochraně osobních údajů – komentář*, Praha: C. H. Beck, 2012, xvii, 516 p. ISBN 978-80-7179-226-0.

Kybic, P. K otázce použití odposlechu a záznamu telekomunikačního provozu jako důkazu v jiné trestní věci, *Trestněprávní revue*, 2002, Vol. 1, No. 4, pp. 114-117. ISSN 1213-5313.

Pokorný, L. *Zpravodajské služby*, Praha: Auditorium, 2012, 150 p. ISBN 978-80-87284-21-6.

Polčák, R. *Internet a proměny práva*, Praha: Auditorium, 2012, 388 p. ISBN 978-80-87284-22-3.

Polčák, R. Púry, F., Harašta, J. et al. *Elektronické důkazy v trestním řízení*, Brno: Masarykova univerzita, 2015, 253 p. ISBN 978-80-210-8073-7.

Polčák, R. Informace a data v právu, *Revue pro právo a technologie*, 2016, Vol. 7, No. 13, pp. 67-91. ISSN 1804-5383.

Polčák, R. Kybernetická bezpečnost jako fenomén českého práva, *Revue pro právo a technologie*, 2015, Vol. 6, No. 11, p. 95-149. ISSN 1804-5383.

Púry, F. Posílení ochrany informací v trestním řízení, *Právní rozhledy*, 2009, Vol. 17, No. 7, p. II. ISSN 1210-6410.

Schwartz, P. The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 1989, *American Journal of Comparative Law*, Vol. 37, No. 4, pp. 675-701. ISSN 0002-919X.

Smejkal, V. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku, *Trestněprávní revue*, 2013, Vol. 2, No. 6, pp. 161-166. ISSN 1213-5313.

Smejkal, V. Ochrana dat advokátů v elektronických úložištích, *Bulletin advokacie*, 2015, No. 3, pp. 15-22. ISSN 1210-6348.

Smejkal, V. *Kybernetická kriminalita*, Plzeň: Aleš Čeněk, 2015, 636 p. ISBN 978-80-7380-501-2.

Šámal, P. et al. *Trestní zákoník – komentář II. § 140-421*, Praha: C. H. Beck, 2009, pp. v-xiv, 1451-3586. ISBN 978-80-7400-428-5.

Šámal, P. et al. *Trestní řád: komentář*. 7., extended release, Praha: C. H. Beck, 2013, xxii, 1898 p. ISBN 978-80-7400-465-0.

Tittlova, M. *Korupcia: Vybrané kriminologické a trestnoprávne aspekty*. Bratislava: Wolters Kluwer, 2015, 258 p. 978-80-8168-264-3.

Vangeli, B. Zákon o Policii České republiky. Commentary. 2. Edition. Praha: C. H. Beck, 2014, 483 s. ISBN 978-80-7400-543-5.

Vantuch, P. Nová úprava odposlechu v trestním řádu od 1. 7. 2008. *Bulletin advokacie*, 2008, No. 10, pp. 28-32. ISSN 1210-6348.

Viktoryova, J. Turek, L. Evidence Admissibility in Pre-trial Proceedings. *Notitiae ex Academia Bratislavensi Iurisprudentiae,* 2009, Vol. 3, No. 2, pp. 7-15. ISSN 1337-6810.

Reports and Opinions

Analysis of tapping and recording of telecommunication traffic. Police Presidium of the Czech Republic. 2014. Online: http://www.mvcr.cz/soubor/ppr-102-31-cj-2014-990390-analyza-odposlechu-a-sledovani-za-rok-2013-pdf.aspx.

EDRI.prg. Slovakia: Mass surveillance of citizens is unconstitutional. Online: https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/.

General Prosecution of Slovak Republic. Annual Report 2013. Online: http://www.genpro.gov.sk/spravy-o-cinnosti-12b7.html.

Husovec, M., Lukic, M. *The quest for privacy in Slovakia: The case of data retention*. 2014. Online: https://www.giswatch.org/sites/default/files/the_quest_for_privacy_in_slovakia.pdf.

NASES. Cyber Security Concept of the Slovak Republic. Online: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1.

Opinion of IT Security Experts on the Clarification of the Amendment to the Criminal Code (Názor odborníků z oblasti ochrany informačních systémů k upřesnění návrhu trestního zákoníku), published online 11. 10. 2015. Online: http://itpravo.cz/index.shtml?x=694071.

Parliamentary Committee for Defence and Security. Annual Report 2013. Online: http://www.nrsr.sk/dl/Browser/Committee?committeeExternalId=125.

Slovak Intelligence Service. Annual Report. Online: http://www.sis.gov.sk/for-you/sis-annual-report.html.

The Concept of Cybersecurity in Slovak Republic. Government materials. Online: https://lt.justice.gov.sk/Attachment/Vlastný%20materiál_docx.pdf?instEID=-1&attEID=75645&docEID=413095&matEID=7996&langEID=1&tStamp=20150218154455240.

Binding Guidelines and Opinions

Binding guideline of the Police President No. 30/2009 Sb. on the tasks in criminal proceedings. Online: http://www.pecina.cz/files/pokyn2.pdf.

Explanatory Opinion of the Supreme Public Prosecutor's Office No. 4/2005. The Supreme Public Prosecutor's Office, SL 788/2004, The Collection of the Explanatory Opinions of the Supreme Public Prosecutor's Office. Online: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2005/stanovisko%204-2005.pdf.

General Instruction of the Supreme Public Prosecutor No. 8/2009, on criminal proceedings. Online: http://www.nsz.cz/images/stories/PDF/POP/trest/1_SL_902-205_2.pdf.

Opinion No. 1/2015 of the Supreme Public Prosecutors Office, on the harmonization of interpretation of laws dealing with access to mobile devices and other storage media, including the content of e-mail inboxes. Online: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

Court Decisions

Czech court decisions

Decision of the Constitutional Court file number II. ÚS 6/93, N 22/1 SbNU 159, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number Pl. ÚS 4/94, 214/1994 Sb., N 46/2 SbNU 57, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number II. ÚS 502/2000, N 11/21 SbNU 83, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number IV.ÚS 412/04, N 223/39 SbNU 353, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number III. ÚS 501/04, N 42/36 SbNU 445, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number II. ÚS 143/06, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number II. ÚS 615/06, N 88/45 SbNU 291, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number II.ÚS 789/06, N 150/46 SbNU 489, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number I. ÚS 3038/07, N 46/48 SbNU 549, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number II. ÚS 2806/08, N 15/56 SbNU 143, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number III. ÚS 3221/09, N 197/58 SbNU 741, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number Pl. ÚS 24/10, 94/2011 Sb., N 52/60 SbNU 625, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number I. ÚS 22/10, N 77/57 SbNU 43, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number Pl. ÚS 24/11, 43/2012 Sb., N 217/63 SbNU 483, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number III. ÚS 2661/12, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number Pl. ÚS 47/13, N 76/73 SbNU 351, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number III. ÚS 3844/13, N 201/75 SbNU 259, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number III. ÚS 3988/13, U 5/72 SbNU 583, online: http://nalus.usoud.cz.

Decision of the Constitutional Court file number I. ÚS 1638/14, online: http://nalus.usoud.cz.

Decision of the Supreme Court file number 7 Tz 9/2000. Online: nsoud.cz.

Decision of the Supreme Court file number 2 To 144/03. Available in beck-online [legal information system].

Decision of the Supreme Court file number 11 Tz 129/2006. Online: nsoud.cz.

Decision of the Supreme Court file number 5 Tdo 459/2007, No. 7/2008 Sb. tr. rozh. Online: nsoud.cz.

Decision of the Supreme Court file number 5 Tdo 572/2009. Online: nsoud.cz.

Decision of the Supreme Court file number 4 Pzo 1/2010. Online: nsoud.cz.

Decision of the Supreme Court file number 4 Pzo 2/2010. Online: nsoud.cz.

Decision of the Supreme Court, file number 4 Pzo 3/2011-37. Online: nsoud.cz.

Decision of the Supreme Court file number Tpjn 304/2012, No. 54/2013 Sb. tr. rozh. Online: nsoud.cz.

Decision of the Supreme Court file number 8 Tdo 908/2013. Online: nsoud.cz.

Decision of the High Court in Prague file number 2 To 73/2000. Available in beck-online [legal information system].

Decision of the High Court in Prague file number 4 To 3/01. Available in beck-online [legal information system].

Decision of the High Court in Prague file number 2 To 139/2005. Available in beck-online [legal information system].

Decision of the Regional Court in České Budějovice, file number 4 To 354/94. Available in beck-online [legal information system].

Decision of the Regional Court in Brno file number C 45/2007-121. Available in beck-online [legal information system].

Decision of the City court in Prague file number No. 42 T 8/2013, online: http://www.pecina.cz/files/Rozsudek_MS-P_30. 4. 2014.pdf.

Interim decision of the City Court in Prague file number Nt 615/2014, online: http://www.scribd.com/doc/235322741/Nt-615-2014.

Slovak court decisions

Decision of the Slovak Constitutional Court file number II. ÚS 152/08. Online: http://portal.concourt.sk/.

Decision of the Slovak Constitutional Court file number Pl. ÚS 3/00. Online: http://portal.concourt.sk/.

Decision of the Slovak Constitutional Court file number I. ÚS 274/05-73. Online: http://portal.concourt.sk/.

Decision of the Slovak Constitutional Court file number Pl. ÚS 3/09. Online: http://portal.concourt.sk/.

Decision of the Slovak Constitutional Court file number I. ÚS 114/2012. Online: http://portal.concourt.sk/Zbierka/2012/29_12s.pdf.

Decision of the Slovak Constitutional Court file number Pl. ÚS 10/2014. Online: http://fra.europa.eu/en/caselaw-reference/slovakia-constitutional-court-slovak-republic-pl-s-102014.

Decision of Supreme Court of the Slovak Republic file number 3 To2/2011. Online: http://www.supcourt.gov.sk.

Decisions of the Court of Justice of European Union and European Court of Human Rights

A. v. France, decision from 23 November 1993, Application No. 14838/89. Online: http://hudoc.echr.coe.int/.

Klass and others v. Germany, decision from 6 September 1978, Application No. 5029/71. Online: http://hudoc.echr.coe.int/.

APPENDIX: COLLECTION OF RELEVANT LEGAL PROVISIONS

Constitutional Act No. 1/1993 Sb., Constitution of the Czech Republic[1]

Article 2

(1) All state authority emanates from the people; they exercise it through legislative, executive, and judicial bodies.

(2) A constitutional act may designate the conditions under which the people may exercise state authority directly.

(3) State authority is to serve all citizens and may be asserted only in cases, within the bounds, and in the manner provided for by law.

(4) All citizens may do that which is not prohibited by law; and nobody may be compelled to do that which is not imposed upon them by law.

Article 3

The Charter of Fundamental Rights and Basic Freedoms forms a part of the constitutional order of the Czech Republic.

Article 10

Promulgated international agreements ratified by the Parliament and binding the Czech Republic are part of law; if the agreement differs from the Act, international agreement shall be used.

Resolution of the Praesidium of Czech National Council No. 2/1993 Sb., Charter of Fundamental Rights and Freedoms[2]

Article 7

(1) Inviolability of the person and of privacy is guaranteed. It may be limited only in cases specified by law.

---

1 Informal translation provided by the Czech Constitutional court. Online: http://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/Ustava_EN_ve_zneni_zak_c._98-2013.pdf

2 Informal translation provided by the Czech Constitutional court. Online: http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Pravni_uprava/AJ/Listina_English_version.pdf.

Article 10

(2) Everybody is entitled to protection against unauthorized interference in his or her personal and family life.

(3) Everybody is entitled to protection against unauthorized gathering, publication or other misuse of his or her personal data.

Article 11

(1) Everybody has the right to own property. The ownership right of all owners has the same statutory content and enjoys the same protection, inheritance is guaranteed.

Article 13

Nobody may violate secrecy of letters and other papers and records whether privately kept or sent by post or in another manner, except in cases and in a manner specified by law. Similar protection is extended to messages communicated by telephone, telegraph or other such facilities.

Act No. 40/2009 Sb., the Criminal Code[3]

Section 12

Principle of Legality and Principle of Subsidiarity of Criminal Repression

(1) Only criminal law shall define criminal offences and prescribe criminal sanctions that may be imposed for their commission.

(2) Criminal liability of an offender and criminal consequences associated with it may only be applied in socially harmful cases where application of liability according to other legal regulations does not suffice.

Section 20

Premeditation

(1) Conduct that is based in an intentional creation of conditions for the commission of a particularly serious crime (Section 14 Subsection 3), especially in its organisation, the acquisition or adaptation of the means or instruments for its commission, in conspiracy, unlawful assembly, in the instigation or aiding of such a crime, shall be deemed a premeditation only if the criminal law applicable for a specific criminal offence expressly stipulates for it and an attempt or completion of a particularly serious crime did not occur.

3 Informal translation taken from the European Judicial Training Network.

(2) Premeditation is punishable pursuant to the criminal penalty set out for a particularly serious crime to which it leads, unless the criminal law stipulates otherwise.

(3) Criminal liability for the premeditation to commit a particularly serious crime shall expire if an offender voluntarily waived further conduct towards the commission of a particularly serious crime and

a) removed the risk to an interest protected by criminal law which occurred due to the attempted premeditation, or

b) reported the premeditation to commit a particularly serious crime at a time when the risk to an interest protected by criminal law which occurred due to the attempted premeditation could still be removed; reporting must be performed to the public prosecutor or the police authority. A soldier may report it to their commander.

(4) If there are several persons involved in an act, the criminal liability for the premeditation is not void in the case of an offender who acted in such manner, despite their timely reporting or earlier participation in such act, if it is completed by other offenders.

(5) The provisions of Subsection 3 and 4 shall have no effect on the criminal liability of an offender for any other committed criminal offence which they have already committed by their conduct pursuant to Subsection 1.

Section 21

Attempt

(1) Any conduct that leads directly to the completion of a criminal offence and which the offender committed with the intention of the commission of a criminal offence, if the completion of the criminal offence did not occur is defined as an attempt to commit a criminal offence.

(2) An attempted criminal offence shall be punishable under the criminal penalty set for a completed criminal offence.

(3) Criminal liability for an attempted criminal offence shall expire if an offender voluntarily waived further conduct leading to the completion of a criminal offence and

a) removed the risk to an interest protected by criminal law which occurred due to the attempted criminal offence, or

b) reported the attempted criminal offence at a time when the risk to an interest protected by criminal law which occurred due to an attempted criminal offence could still be removed; reporting must be performed to the public prosecutor or the police authority. A soldier may report it to their commander.

(4) If there are several persons involved in an act, the criminal liability for an attempt is not void in the case of an offender who acted in such manner, despite their timely reporting or earlier participation in such act, if it is completed by other offenders.

(5) The provisions of Subsection 3 and 4 shall have no effect on the criminal liability of an offender for any other completed criminal offence which they have already committed by their conduct pursuant to Subsection 1.

Section 28

Extreme Emergency

(1) An act, which is otherwise criminal, whereby a person tries to avert a risk imminently threatening an interest protected by criminal law, is not a criminal offence.

(2) Extreme emergency shall not apply if such risk could be otherwise averted under the given circumstances, or if the consequences caused are evidently equally serious or even more serious than those imminent, or if the person at risk was obliged to endure them.

Section 29

Self Defence

(1) An act, which is otherwise criminal, whereby a person tries to avert an imminently threatening or continuous assault on an interest protected by criminal law, is not a criminal offence.

(2) Self defence shall not apply if the defence was clearly disproportionate to the method of the assault.

Section 182

Violating Confidentiality of Messages

(1) Whoever intentionally violates the confidentiality

a) of a closed letter or other document during the provision of postal services or transported by other transport services or transport facilities,

b) of data, text, voice, audio or video messages sent via electronic communications networks and attributable to an identified subscriber or user who receives the message, or

c) of non-public transmission of computer data into a computer system, from or within which, including electromagnetic radiation from a computer system, transferring such computer data, shall be punished by a prison sentence of up to two years or punishment by disqualification.

(2) Whoever with the intention to cause damage to another person or to procure an unauthorised benefit for themselves or another person

a) reveals the secret of which they learned from the document, telegram, telephone call or electronic transmission through a communications network, which was not intended for them, or

b) takes advantage of such secrets, shall be similarly punished.

(3) An offender shall be punished by a prison sentence of six months to three years or punishment by disqualification, if,

a) they committed an act referred to in Subsection 1 or 2 as a member of an organised group,

b) they committed such an act out of reprehensible motives,

c) they caused substantial damage by committing such an ac, or

d) they committed such an act with the intention of gaining a substantial benefit for themselves or someone else.

(4) An offender shall be punished by a prison sentence of one to five years or a monetary penalty, if,

a) they committed an act referred to in Subsection 1 or 2 as an official person,

b) they caused large-scale damage by committing such an act, or

c) they committed such an act with the intention to procure another large-scale benefit for themselves or someone else.

(5) An employee of postal services, telecommunications services or computer system or anyone else engaged in communication activities who

a) commits an act referred to in Subsection 1 or 2,

b) intentionally allows another person to commit such an act, or

c) amends or suppresses the document contained in a postal consignment or transported by transport facilities or a report filed by non-public transmission of computer data, telephone, telegram, or in another similar manner, shall be punished by a prison sentence of one to five years, a monetary penalty or punishment by disqualification.

(6) An offender shall be punished by a prison sentence of three to ten years, if,

a) they caused large-scale damage by committing an act referred to in Subsection 5, or

b) they committed such an act with the intention to procure another large-scale benefit for themselves or someone else.

Section 183

Breach of Confidentiality of Documents and other Privately Kept Documents

(1) Whoever violates the confidentiality of documents or other documents, photographs, film or other recordings, computer data, or other documents kept privately by another person without authorisation, by publishing, making them available to third parties, or otherwise uses them, shall be punished by a prison sentence of up to one year, a punishment by disqualification, or forfeiture of items or other assets.

(2) An offender shall be punished by a prison sentence of up to two years, a punishment by disqualification, or forfeiture of items or other assets, if they committed an act referred to in Subsection 1 with the intention to procure material or other benefits for themselves or someone else, to cause damage to another person or other serious damage, or to jeopardise their social esteem.

(3) An offender shall be punished by a prison sentence of six months to five years or a monetary penalty, if,

a) they committed an act referred to in Subsection 1 as a member of an organised group,

b) they committed such an act against another person for their actual or perceived race, ethnicity, nationality, political belief, religion, or because they are actually or allegedly non-religious,

c) they caused substantial damage by committing such an act, or

d) they committed such an act with the intention of gaining a substantial benefit for themselves or someone else.

(4) An offender shall be punished by a prison sentence of two to eight years, if,

a) they caused large-scale damage by committing an act referred to in Subsection 1, or

b) they committed such an act with the intention to procure another large-scale benefit for themselves or someone else.

Section 230

Unauthorised Access to Computer Systems and Information Media

(1) Whoever overcomes security measures and thus gains access to a computer system or part thereof without authorisation shall be punished by a prison sentence of up to one year, punishment by disqualification, or forfeiture of items or other assets.

(2) Any person who gains access to a computer system or information medium and

a) uses data stored in a computer system or information media without authorisation,

b) 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,

c) forges or alters data stored in a computer system or information media so as to be considered authentic and according to them it was treated as if it was authentic data, notwithstanding the fact whether the data is directly readable and understandable, or

d) 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,

shall be punished by a prison sentence of up to two years, punishment by disqualification, or forfeiture of items or other assets.

(3) An offender shall be punished by a prison sentence of six months to three years, punishment by disqualification, or forfeiture of items or other assets, if they committed an act referred to in Subsection 1 or 2

a) with the intention to cause damage to another person or to obtain an unauthorised benefit for themselves or another person, or

b) with the intention to restrict the functionality of a computer system or other technical equipment for data processing without authorisation.

(4) An offender shall be punished by a prison sentence of one to five years or a monetary penalty, if,

a) they committed an act referred to in Subsection 1 or 2 as a member of an organised group,

b) they caused substantial damage by committing such an act,

c) they caused substantial interference in the activities of the State Administration body, local government, court, or another public authority by committing such an act,

d) they procured a substantial benefit by committing such act for themselves or another person, or

e) they caused serious interference in the activity of a legal entity or natural person who is an entrepreneur by committing such an act.

(5) An offender shall be punished by a prison sentence of three to eight years, if,

a) they caused large-scale damage by committing an act referred to in Subsection 1 or 2, or

b) they procured another large-scale benefit by committing such act for themselves or another person.

Section 231

Measures and Possession of Access Devices and Computer System Passwords and other such Data

(1) A person who intends to commit a criminal offence of violating confidentiality of messages under Section 182 Subsection 1 Paragraph b), c) or a criminal offence of unauthorised access to computer systems and information media under Section 230 Subsection 1, 2 produces, puts into circulation, imports, exports, transports, offers, provides, sells, or otherwise makes available, procures for themselves or another person or possesses

a) a device or its component, process, instrument or any other means, including a computer programme, designed or adapted for unauthorised access to electronic communications networks, a computer system or part thereof, or

b) 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,

shall be punished by a prison sentence of up to one year, forfeiture of items or other assets, or punishment by disqualification.

(2) An offender shall be punished by a prison sentence of up to three years, punishment by disqualification, or forfeiture of items or other assets, if,

a) they committed an act referred to in Subsection 1 as a member of an organised group, or

b) they procured a substantial benefit by committing such act for themselves or another person.

(3) An offender shall be punished by a prison sentence of six months to five years if they procured another large-scale benefit for themselves or another person by committing an act referred to in Subsection 1.

Section 232

Damage to Computer Systems and Information Medium Records and Intervention into the Computer Equipment out of Negligence

(1) A person who violates, out of gross negligence, an obligation arising from their employment, occupation, position or function or one imposed by law, or one that is contractually assumed, and

a) destroys, damages, alters or renders unusable the data stored in a computer system or information media, or

b) makes an intervention into the hardware or software of the computer or other technical data processing equipment,

and thus causes substantial damage to the stranger's property, shall be punished by a prison sentence of up to six months, punishment by disqualification, or forfeiture of items or other assets.

(2) An offender shall be punished by a prison sentence of up to two years, punishment by disqualification, or forfeiture of items or other assets if they caused large-scale damage by committing an act referred to in Subsection 1.

Section 317

Endangering Classified Information

(1) Whoever pries information classified under another legal regulation with the aim to disclose it to an unauthorised person, whoever with such an aim collects data containing classified information, or whoever discloses such classified information intentionally to any unauthorised person, shall be punished by a prison sentence of up to three years or punishment by disqualification.

(2) An offender shall be punished by a prison sentence of two to eight years, if,

a) they intentionally disclosed classified information to any unauthorised person under another legal regulation classed as "Top Secret" or "Secret",

b) they committed an act referred to in Subsection 1, though the obligation to protect the classified information was specifically imposed upon them, or

c) they procured a substantial benefit for themselves or another person, or they caused substantial damage or a particularly serious consequence by committing such act.

(3) An offender shall be punished by a prison sentence of five to twelve years, if a) the act referred to in Subsection 1 relates to classified information from the area of security of the defensibility of the Czech Republic classed in another legal regulation as "Top Secret", or

b) they committed such act during a state of national emergency or war.

(4) Premeditation is punishable.

Section 318

Endangering Classified Information out of Negligence

Whoever, out of negligence, causes the disclosure of classified information under another legal regulation classed as "Top Secret" or "Secret" shall be punished by a prison sentence of up to three years or punishment by disqualification.

Section 329

Abuse of Powers of an Official Person

(1) An official person who, with the intention to cause damage or other serious harm to another person or to procure an unauthorised benefit for themselves or another person

a) performs their powers in a manner contrary to another legal regulation,

b) exceeds their powers, or

c) fails to meet an obligation under their powers,

shall be punished by a prison sentence of one to five years or punishment by disqualification.

(2) An offender shall be punished by a prison sentence of three to ten years, if,

a) they procured a substantial benefit for themselves or another person by committing an act referred to in Subsection 1,

b) they committed such an act on another person for their actual or perceived race, ethnicity, nationality, political belief, religion, or because they are actually or allegedly non-religious,

c) they caused substantial disruption to the activities of a public administration body, local government, court or another public authority by committing such an act,

d) they caused serious disruption to the activities of a legal entity or natural person who is an entrepreneur by committing such an act,

e) they committed such an act while abusing the vulnerability, addiction, anxiety, cognitive weakness, or inexperience of another person, or

f) they caused substantial damage by committing such an act.

(3) An offender shall be punished by a prison sentence of five to twelve years or forfeiture of property, if,

a) they procured another large-scale benefit for themselves or another person by committing an act referred to in Subsection 1, or

b) they caused large-scale damage by committing such an act.

(4) Premeditation is punishable.

Act No. 141/1961 Sb., on Criminal Procedure (Code of Criminal Procedure)[4]

Section 2

Basic Principles of Criminal Procedure

(1) No person shall be prosecuted other than for legitimate reasons and in a manner as stipulated by this Act.

(2) A person against whom a criminal procedure is carried out may not be perceived as guilty until the final convicting judgment of the court pronounces them as guilty.

(3) The public prosecutor is obliged to prosecute all criminal offences of which they learn, unless the law or a promulgated international treaty to which the Czech Republic is bound stipulates otherwise.

(4) Unless this Act stipulates otherwise, the law enforcement authorities act ex officio. Criminal cases must be dealt with expeditiously without undue delays; the most expeditious procedure shall be taken in particular for custody matters and the matters in which property was impounded if this

4 Informal translation provided by the Ministry of Justice.

is required with regard to the value and nature of the impounded property. Criminal cases shall be dealt with with a full investigation of rights and freedoms guaranteed by the Charter of Fundamental Rights and Freedoms and by international treaties on human rights and fundamental freedoms that the Czech Republic is bound by; when conducting acts of criminal proceedings, the rights of persons that such acts affect may be intervened only when justified by law and to the extent necessary to ensure the purpose of criminal proceedings. The law enforcement authorities shall not take the content of petitions affecting the performance of such obligations into account.

(5) Law enforcement authorities act in accordance with their rights and obligations under this Act and with the assistance of the parties so as to duly establish the facts of the case of which no reasonable doubt exists and to the extent that is necessary for their decisions. A confession of the accused shall not relieve the law enforcement authorities from the obligation to examine all the relevant circumstances of the case. During the preliminary hearings, the law enforcement authorities shall ascertain all the circumstances for and against the person against whom the proceeding is pending with the same care and in the manner provided by this Act even without petitions of the parties to an action. In proceedings before the court the public prosecutor and the accused may support their position with the proposal and submission of evidence. The public prosecutor must prove the guilt of the defendant. However, this does not relieve the court of the obligation to provide additional evidence to the extent required for their decision.

(6) Law enforcement authorities shall review the evidence according to their conviction based on careful consideration of all the circumstances of the case separately and as a whole.

(7) All law enforcement authorities shall cooperate with public interest groups and utilise their educational activities.

(8) A criminal prosecution before the courts is only possible on the basis of an indictment, a petition for punishment or a petition for approval of an agreement on the declaration of guilt and acceptance of punishment (hereinafter referred to as an "agreement on guilt and punishment") served by the public prosecutor. A bill of indictment in proceedings before the court is represented by the public prosecutor.

(9) In criminal proceedings before the court, decisions are made by the court or a single judge; the presiding judge or a single judge decides alone only if so expressly stipulated by the law. Should the decision during a preliminary hearing be made by a court in the first instance, then such decisions shall be made by a judge.

(10) Criminal cases are heard in public before the court so that citizens may observe and participate in hearing. At the main trial and public hearing, the public may be excluded only in cases expressly stipulated for in this Act or in a special Act.

(11) Proceedings before the courts are oral; the testimony of witnesses, experts and the accused are normally undertaken through an interrogation.

(12) When deciding during a main trial, as well as during public, custody and closed hearings, the court may only take into account evidence that was given during such proceedings.

(13) The person against whom criminal proceedings have been initiated must be instructed in every stage of the proceedings in an appropriate and comprehensible manner as to their rights granting them the full use of defence and that they may choose their defence counsel; all law enforcement authorities are required to enable them to exercise their rights.

(14) Law enforcement authorities conduct the proceedings and produce decisions in the Czech language. Any person who declares that they do not speak Czech is entitled to speak their mother tongue or a language that they indicate they can speak to the law enforcement authorities.

(15) At every stage of the proceedings the law enforcement authorities are obliged to make it possible for the victim to fully exercise their rights and are also obliged to instruct the victim of the victim's rights in an appropriate and comprehensible manner under the law so that the victim can achieve satisfaction of their claims; the proceedings must be conducted with the required consideration for the victim and while being duly regardful of their person.

Section 8

(1) Public authorities, legal entities and natural persons are required to comply with letters of request from law enforcement authorities for the

performance of their actions without undue delay and unless a special regulation stipulates otherwise, to comply without payment. Furthermore, public authorities are also obliged to immediately notify the public prosecutor or the police authorities of facts indicating that a criminal offence has been committed.

(2) If the criminal proceedings require a proper investigation of the circumstances suggesting that a criminal offence has been committed or to assess the circumstances of the accused during court proceedings or for the enforcement of a decision, the public prosecutor and, after the indictment or a punishment petition, the presiding judge may request information that is subject to banking secrecy and data from the security register. Pursuant to Section 180 of the Penal Code, the law enforcement authority may request individual data obtained under a special Act for statistical purposes during the criminal proceedings. The conditions under which the law enforcement authority may require the data obtained in the administration of taxes are stipulated under a special Act. Data obtained under this provision may not be used for a purpose other than the criminal proceedings for which such data was requested.

(3) For the reasons as stated in Subsection 2, the presiding judge may, and upon the proposal of the public prosecutor during a preliminary hearing, order the surveillance of the bank accounts or accounts of persons entitled to the records of investment instruments under a special Act for a maximum period of six months. If the reason for which the surveillance of an account was ordered exceeds this time, it may be extended upon the order of a judge from a court of higher instance and, during preliminary hearing, upon the proposal of the public prosecutor of the County Court judge for a further six months, and such prolongation can be performed repeatedly. Information obtained under this provision may not be used for a purpose other than the criminal proceedings for which it was obtained.

(4) The performance of obligations under Subsection 1 may be rejected with reference to the obligation to maintain the secrecy of classified information protected by a special Act or imposed by the State or the recognised duty of confidentiality; this does not apply,

a) if the person who has the obligation would otherwise risk criminal prosecution for the failure to notify or prevent a criminal offence, or

b) in executing the request of a law enforcement authority with regards to a criminal offence, where the requested person is also the reporter of the criminal offence.

The State recognised obligation of confidentiality under this Act does not consider such obligation the scope of which is not defined by law but instead arises from a legal action taken under the law.

(5) Unless a special Act stipulates the conditions under which information may be disclosed for the purpose of criminal proceedings that are deemed classified pursuant to such Act or which is subject to an obligation of secrecy, such information may be requested for criminal proceedings upon the prior consent of the judge. This does not affect the obligation of confidentiality of an attorney under the Advocacy Act.

(6) The provisions of Subsection 1 and 5 shall not affect the obligation of confidentiality imposed on the basis of a declared international treaty to which the Czech Republic is bound.

It is to be noted that recognised by criminal procedural law are only those secrecy duties that are laid down by statutory law (not those that are e.g. established between parties by a non-disclosure agreements).

Section 8c

Pursuant to Section 88 no person shall disclose information on the court order or interception performance and recording of telecommunications traffic without the consent of persons whom such information concerns or information derived thereof, data on telecommunications traffic detected on the basis of an order under Section 88a, or information obtained by the surveillance of people and items under Section 158d Subsection 2 and 3, if such information allows the identification of the person and if such were not used as evidence in proceedings before the court.

Section 12

Interpretation of Certain Terms

(2) Police authorities mean

a) bodies of the Police of the Czech Republic,

b) General Inspection of Security Forces in proceedings on criminal offences committed by members of the Police of the Czech Republic, members of the Prison Service of the Czech Republic, customs officers or employees of the Czech Republic classified to work in the Police of the Czech Republic, or on criminal offences by employees of the Czech Republic classified to work in the Prison Service of the Czech Republic or in the Customs Administration of the Czech Republic which were committed in connection with fulfilment of their employment duties,

c) appointed bodies of the Prison Service of the Czech Republic in proceedings on criminal offences of persons serving detention, a prison sentence or security detention that were committed in a custodial prison, prison or institute for the execution of security detention,

d) appointed customs authorities in proceedings on criminal offences committed by a breach of customs regulations or regulations on the import, export or transit of goods, even in cases of criminal offences by members of the armed forces or security forces, and by a breach of laws in the placement and purchase of goods in Member States of the European Communities if such goods are transported across the national borders of the Czech Republic, and in cases of tax infringements, where the customs authorities manage tax under special legal regulations,

e) appointed bodies of the Military Police in proceedings on criminal offences of members of the armed forces and persons who commit a criminal activity against members of the armed forces in military facilities, against military facilities, military material or other property of the State that is to be managed by the Ministry of Defence,

f) appointed authorities of the Security Information Service in proceedings on criminal offences committed by members of the Security Information Service,

g) appointed authorities of the Office for Foreign Relations and Information in proceedings on criminal offences committed by members of the Office for Foreign Relations and Information,

h) appointed authorities of Military Intelligence in proceedings on criminal offences committed by members of Military Intelligence,

i) appointed authorities of the General Inspection of Security Forces in proceedings on criminal offences committed by members of the General Inspection of Security Forces or on the criminal offences of employees of the Czech Republic classified to work in the General Inspection of Security Forces.

This does not affect the entitlement of the public prosecutor under Section 157 Subsection 2, Paragraph b). Unless stipulated otherwise, the listed authorities are entitled to all acts of criminal procedure falling under the scope of the police authority.

Section 30

(1) The judge or an associate judge, public prosecutor, police authority or a person employed by it who gives way to a reasonable doubt that in relation to the case or persons who are directly related to it, to their attorneys, legal representatives and agents, or due to their relationship to other law enforcement authorities they cannot make impartial decisions, then they are excluded from carrying out acts of criminal proceedings. Actions that were taken by the excluded persons may not be the basis for decisions in the criminal proceedings.

(2) A judge or an associate judge is also excluded from carrying out acts of criminal proceedings if they were active in the case as a public prosecutor, police authority, community representative, defence counsel or as an agent of the party to an action and the victim. After the indictment or petition for approval of an agreement on guilt and punishment is filed, the judge who in the matter under discussion in the preliminary hearing ordered the home search or search of other premises and land or issued a detention order or warrant for arrest or decided on the custody of the person against whom an indictment was subsequently filed or with whom an agreement on guilt and punishment was concluded, is excluded from carrying out acts of criminal proceedings.

(3) The judge or an associate judge who participated in the decision making at a lower court are also excluded from the decision making process at the higher court and vice versa. The public prosecutor who made the contested decision or gave their consent or order is excluded from the decision making process on the issue of a complaint to the higher authority.

(4) The judge who took part in the decision making process of the earlier proceedings is excluded from the proceedings on the review of the order for the interception and recording of telecommunications traffic. The judge who participated in the decision making process on the review of the order for the interception and recording of telecommunications traffic is further excluded from the decision making process of the subsequent proceedings.

Section 55

General Provisions for Transcript Recording

(1) Unless the law stipulates otherwise, at any action of criminal proceedings a transcript is recorded, usually during an action or immediately after, which must include

a) the name of the court, public prosecutor or other law enforcement authority,

b) the place, time and subject of an action,

c) name and surname of officials and their functions, name and surname of the parties present, the name, surname and address of the legal representatives, legal counsel and agents who participated in the action, and in the case of the victim and the accused also the address that is specified for the purpose of delivery, and other data necessary to establish or verify identities, including date of birth or birth certificate numbers,

d) brief and concise statements of the course of an action which would be seen as preserving the statutory provisions governing the conduct of an action, essential contents of the decisions announced during an action, and if a copy of the decision was delivered immediately after reaching the decision, and the confirmation of this service; if there is a literal transcript of the person's statement, it is necessary to indicate such in the transcript accordingly so that it is possible to safely identify the beginning and end of the literal transcript,

e) petitions of the parties, issued instructions, and/or an expression of the instructed persons,

f) objections of the parties or the persons interviewed during the execution of an action or the content of the transcript.

(2) Should the identified condition indicate that the witness or persons close to them appear to be under threat of bodily harm or any other serious risk of violation of their fundamental rights in relation to their testimony and witness protection can not be safely ensured by some other means, the law enforcement authorities shall take steps to conceal the identity of the witness; the name and surname and other personal information is not recorded in the transcript but are kept separate from the criminal file and only law enforcement authorities may gain access to such details for the purpose of the case. A witness shall be instructed on the right to request confidentiality of their identity and must sign the transcript under an assumed name and surname under which they are further recorded. If the protection of such persons is required, law enforcement authorities must take all necessary steps without undue delay. A special manner to protect witnesses and persons close to them is stipulated by a special Act. If the reasons for the confidentiality of identity and a separate record of personal data of witnesses has expired, the authority responsible for the legal proceedings at the time shall revoke the level of classification of information, attach the information to the criminal file, and the identity and details of the witnesses cease to be classified; this does not apply to the classified identity of persons listed in Section 102a.

(3) The transcript drawn up on the conflict shall include literal testimonies of the confronted persons, as well as the wording of questions and answers; and the circumstances that are important in terms of the purpose and implementation of the confrontation. The transcript is drawn up about the recognition and it must include detailed circumstances under which the recognition was performed, in particular the order in which the persons or items are shown to the suspect, accused or witness, the time and conditions of their observations and their opinions; the recognition conducted in the preliminary hearing is usually video recorded. The transcript drawn up about the investigative attempt, the reconstruction and on-site review is necessary

to describe all the circumstances under which these actions were carried out in detail, including their contents and results; if the circumstances of the case do not exclude it, video recordings, sketches, and other appropriate tools shall, if possible, be included in the transcript. Similarly, it is necessary to proceed even if an event when the implementation of other evidence is not explicitly provided by law.

(4) The transcript in the Czech language is drawn up on the testimony of a person even if the questioned person speaks another language; depending on the literal testimony, the reporter or an interpreter shall record the relevant part of the testimonies in the language spoken by the person who testifies.

(5) The correct transcript is guaranteed by the person who performs the operation.

Inspection of Documents

Section 65

(1) The accused, victim and party to an action, their defence counsel and their agents have the right to inspect files, with the exception of the voting record and the personal data of the witnesses in accordance with Section 55 Subsection 2, to make extracts from them and notes, and make copies of files and their parts at own expense. The same right applies to the legal representatives of the accused, victim or the party to an action if they are denied legal capacity or if their legal capacity is restricted. Other people may then do so with the consent of the presiding judge and in criminal proceedings with the consent of the public prosecutor or the police authority only if it is necessary to exercise their rights.

(2) The public prosecutor or the police authority are entitled to inspect the files, along with the other rights referred to in Subsection 1, and they may deny them based on important reasons in the preliminary hearing. The public prosecutor is obligated to urgently review the severity of the grounds on which those rights are denied by the police authority and the request of the person to whom the refusal concerns. These rights can not be denied to the accused and the defence counsel once they have been advised of the possibility to study the files, and when concluding an agreement on guilt and punishment.

(3) Those who had the right to be present to an action can not be denied access to the transcript of such an action. The accused and their legal counsel could not be denied access to the resolution to initiate criminal prosecution (Section 160 Subsection 1).

(4) The rights of public authorities and a national member of Eurojust to access the files under other legal regulations are not established with prejudice to the provisions of the preceding Subsections.

(5) When authorising access to the files, it is necessary to take such steps to preserve the secrecy of the classified information protected by a special Act which is related to the state ordered or recognised confidentiality obligation.

(6) When files are to be inspected, it is necessary to take such measures to prevent access to data that may, under Section 55 Subsection 1 Paragraph c), only be learnt by the law enforcement authorities and officials of the Probation and Mediation Service acting in the matter concerned. Where a person against whom the criminal proceedings are conducted requests notification of such data, Section 55 Subsection 1 Paragraph c) shall apply accordingly.

Section 78

Obligation to Release Property

(1) Those who are carrying a tangible property important to the criminal proceedings are obligated to submit it to the court, public prosecutor, or police authority when prompted; if the purpose of the criminal proceedings requires its securing, they are obligated to release the property when prompted. When prompted, it is necessary to note that if they fail to comply with the call, the property may be removed from them, as well as there being other consequences of non-compliance (Section 66).

(2) The obligation under Subsection 1 shall not apply to an instrument whose content relates to the circumstances of the ban on interrogation, unless there was an exemption from the obligation to keep the matter secret or confidential (Section 99).

(3) The presiding judge and in the preliminary hearing, the public prosecutor or the police authority, are entitled to prompt the release.

(4) Where tangible property to which the rights to be secured are attached was released, the securing of such rights shall take place accordingly under Section 79e.

(5) The person who released the tangible property must not transfer such property to another person or encumber it during the impoundage. Any legal action made contrary to this prohibition is invalid; the court shall take account of such invalidity even without a petition. Such person must be instructed on this.

(6) The law enforcement authority stated in Subsection 3 shall order the person who released the tangible property to notify the law enforcement authority within the term set by such authority whether and who has a pre-emption or other right to the released property or whether the exercise of the right to dispose of the property is restricted in another manner, and such person shall also be advised of the consequences of failure to grant such request within the set term (Section 66); subsequently the law enforcement authority shall notify the impoundage of the tangible property to those persons and authorities about whom the law enforcement authority learns that they have a pre-emption or other right to such property or are conducting proceedings in which the exercise of the right to dispose of such property has been restricted. It shall also notify the authority that keeps a register of such properties under other legal regulations of the property's impoundage without undue delay.

(7) The procedure in the management of impounded tangible properties shall be governed by special legal regulations.

(8) Subsection 4 through 7 shall not apply to tangible properties that were taken into custody by a law enforcement authority in criminal proceedings only in order to take evidence.

Section 79

Seizure of Property

(1) If the tangible property important to the criminal proceedings is not released when those who have it in their possession are prompted, it may be removed from their possession on the warrant of the presiding judge,

and in preliminary hearing, the public prosecutor or police authority. The police authority needs to have the prior approval of the public prosecutor for the issue of such warrant.

(2) If the authority that issued the warrant for the seizure of the tangible property does not seize such property themselves, the police authority shall do so on the basis of the warrant.

(3) Without the prior consent referred to in Subsection 1 the warrant may be issued by the police authority only if prior approval cannot be achieved and the matter cannot be delayed.

(4) A person who is not involved in the matter shall take part in seizing the tangible property.

(5) The transcript of the release and seizure of the tangible property must also contain a sufficiently accurate description of the released or seized property that would make it possible to determine its identity.

(6) The authority that performed the action shall immediately issue a written confirmation of the receipt of the property or a copy of the transcript to the person who released the tangible property or from whom the tangible property was removed, together with a written instruction that they must not transfer the released or removed tangible property to another party or encumber it and that any legal action made contrary to such prohibition is invalid.

(7) Removed tangible property that was not taken into custody by a law enforcement authority in order to take evidence shall be governed accordingly by Section 78 Subsection 4 through 8.

Section 82

Reasons for House and Personal Searches and
Search of Other Premises and Land

(1) A house search can be conducted if there is a reasonable suspicion that a person or property important for criminal proceedings is present in the residence or other premises used for housing or on premises associated with them (residence).

2) Due to the grounds provided for in Subsection 1 a search of non-residential premises (other premises) and land, if not publicly accessible, may be performed.

(3) Personal searches may be performed if there is a reasonable suspicion that someone is carrying property important to criminal proceedings.

(4) A detained person and a person who was arrested or taken into custody may even be inspected if there is a suspicion that they are in possession of a weapon or other property that could endanger their own or someone else's life or health.

Section 88

Interception and Recording of Telecommunications

(1) If criminal proceedings are conducted for a crime for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, for a criminal offence of machinations in insolvency proceedings under Section 226 of the Penal Code, violation of regulations on rules of competition under Section 248 Subsection 1 Paragraph e) and Subsection 2 through 4 of the Penal Code, negotiating advantages during public procurement, tender and auction under Section 256 of the Penal Code, machinations during public procurement and tenders under Section 257 of the Penal Code, machinations at a public auction under Section 258 of the Penal Code, misuse of powers of an official person under Section 329 of the Penal Code or for any other intentional criminal offence for which prosecution is stipulated in a declared international treaty, an order for the interception and recording of telecommunications may be issued if it may be reasonably assumed that facts relevant to the criminal proceedings will be obtained in this way and if there is no other way to achieve such purpose or if its achievement would be otherwise significantly reduced. The Police of the Czech Republic perform the interception and recording of telecommunications for the needs of all law enforcement authorities. The interception and recording of telecommunications between the defence counsel and the accused is inadmissible. If the police authority finds during the interception and recording of telecommunications that the accused has communicated with their defence counsel, they are obliged to immediately destroy the

interception recording and not to use the information learned in this context in any way. The report on the destruction of the record shall be placed in the file.

(2) The presiding judge and, in preliminary proceedings upon the petition of the public prosecutor, the judge, is entitled to warrant the interception and recording of telecommunications. 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 interception and recording of telecommunications must be issued in writing and must be justified, including a specific reference to the applicable international treaty. The order for the interception and recording of the telecommunications service shall include a determined user address or a user device and the user if their identity is known, and the period during which the interception and recording 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 interception and recording of telecommunications shall immediately be forwarded to the police authority. In the preliminary hearing, the judge shall send a copy of the order for the interception and recording of telecommunications to the public prosecutor without undue delay.

(3) The police authority is obliged to continuously assess whether the reasons which led to an order for the interception and recording of telecommunications 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 period referred to in Subsection 2. They will immediately notify the presiding judge in writing, who issued the order for the interception and recording of telecommunications, and in the preliminary hearing, the public prosecutor and the judge.

(4) Based on the assessment of the current course of the interception and, recording 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 interception and recording of telecommunications traffic even repeatedly, however, always only for a maximum period of four months.

(5) The law enforcement authority may, without the order for the interception and recording of telecommunications, order the interception and recording 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), dangerous threats (Section 353 of the Penal Code) or dangerous persecution (Section 354 of the Penal Code), if the user of the intercepted unit agrees to such measure.

(6) If the record of the telecommunications service is to be used as evidence, it is necessary to accompany it with the transcript, giving the place, time, manner and contents of the record, as well as the authority which issued the record. The police authority is obliged to label other records, securely store them so as to protect them against unauthorised misuse, and indicate the place of storage in the transcript. In another criminal case other than the one in which the interception and recording of telecommunications service was performed, the recording may be used as evidence if there is a criminal prosecution in this matter for a criminal offence referred to in Subsection 1, or with the consent of the user by the intercepted station.

(7) If the interception and recording 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 shall destroy the records of the interception after the decision on the extraordinary appeal or after a final conclusion on the matter. The police authority shall send a transcript on the destruction of the record of the interception to the public prosecutor, whose decision finally concluded the matter and in proceedings before the court, to the presiding judge in the first instance, for the record on file.

(8) The public prosecutor or the police authority, 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, shall inform the person referred to in Subsection 2, if known, on the ordered interception and recording of telecommunications service. The information includes the designation of the court that issued an order for the interception and recording of telecommunications service, the duration of the interception 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 interception and recording of telecommunications service to the Supreme Court. The presiding judge of the court in the first instance shall submit the information without undue delay after the final conclusion of the matter, the public prosecutor by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the Attorney General under Section 174a and the police authority by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the public prosecutor under Section 174 Subsection 2 Paragraph e).

(9) The presiding judge, the public prosecutor or the police authority does not submit the information under Subsection 8 in proceedings on a crime committed by an organised group for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, in proceedings on criminal offences committed for the benefit of an organised criminal group, in proceedings for criminal participation in an organised criminal group (Section 361 of the Penal Code), 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, including those referred to in Subsection 6, or if it could lead to threats to national security, life, health, or the rights and freedoms of individuals.

Section 88a

(1) If, for the purposes of criminal proceedings conducted for an intentional criminal offence for which the law sets out a prison sentence with an upper penalty limit of at least three years, for the criminal offence of violating the confidentiality of messages (Section 182 of the Penal Code), for the criminal offence of fraud (Section 209 of the Penal Code), for the criminal offence of unauthorised access to computer systems and information media (Section 230 of the Penal Code), for the criminal offence of procuring and possessing access devices and computer system passwords and other such data (Section 231 of the Penal Code), for the criminal offence of dangerous threats (Section 353 of the Penal Code), for the criminal offence of dangerous persecution (Section 354 of the Penal Code), for the criminal offence of spreading alarming news (Section 357 of the Penal Code), for the criminal offence of encouraging a criminal offence (Section 364 of the Penal Code), for the criminal offence of approving a criminal offence (Section 365 of the Penal Code) or for an intentional criminal offence for which prosecution is stipulated in a proclaimed international treaty binding on the Czech Republic, it is necessary to ascertain data on the telecommunications service that are the subject of a telecommunications secret or that are subject to the protection of personal and intermediation data, and there is no other way to achieve the pursued purpose or if its achievement would be otherwise significantly harder, their release to the public prosecutor or to the police authority shall be ordered by the presiding judge in proceedings before the court and by the judge upon the petition of the public prosecutor in a preliminary hearing. If there are criminal proceedings for a criminal offence the prosecution of which is stipulated in such international treaty, the order for ascertaining data on the telecommunications service must be issued in writing and must be justified, including a specific reference to the proclaimed international treaty. If the request applies to a particular user, their identity must be stated in the order, if known.

(2) The public prosecutor or the police authority by whose decision the matter was finally concluded, and in proceedings before the court the presiding judge of the court of first instance after the final conclusion of the matter, shall inform the user referred to in Subsection 1, if known, of the ordered

ascertainment of data on the telecommunications service. The information shall identify the court which issued the order for the ascertainment of data on the telecommunications service, and detail the period to which such order applied. Such information shall include instructions on the right to submit to the Supreme Court, within six months of receipt of this information, a petition to review the legality of the order for the ascertainment of data on the telecommunications service. The presiding judge of the court of first instance shall submit the information without undue delay after the final conclusion of the matter, the public prosecutor by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the Attorney General under Section 174a, and the police authority by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the public prosecutor under Section 174 Subsection 2 Paragraph e).

(3) The presiding judge, the public prosecutor or the police authority shall not submit the information under Subsection 2 in proceedings on a crime committed by an organised group for which the law stipulates a prison sentence with an upper penalty limit of at least eight years, in proceedings on a criminal offence committed for the benefit of an organised criminal group, in proceedings on the criminal offence of participation in an organised criminal group (Section 361 of the Penal Code), or if the commission of the criminal offence involved several persons and in relation to at least one of them criminal proceedings have not yet been finally concluded or if criminal proceedings are conducted against the person to whom the information is to be submitted, or if providing such information could defeat the purpose of the particular or some other criminal proceedings, or if it could threaten national security, life, health, or the rights or freedoms of individuals.

(4) An order under Subsection 1 is not required if the user of the telecommunications equipment to whom the data on the performed telecommunications service relates gives their approval for the provision of the information.

Section 89

General Provisions

(1) In a criminal prosecution it is required to prove to the necessary extent, in particular:

a) whether an act is seen as a criminal offence,

b) whether the act was committed by the accused or based on what motives,

c) significant factors affecting the assessment of the nature and seriousness of the act,

d) the relevant circumstances to assess the offenders' personal circumstances,

e) the significant circumstances allowing the determination of the consequences, the amount of damage and unjust enrichment, caused by the criminal offence,

f) the circumstances that led to the criminal activity or allowed it to be committed.

(2) Evidence may be anything that may help to clarify matters, in particular the testimonies of the accused and witnesses, expert opinions, items and documents relevant to the criminal proceedings, and examinations. Each party may seek, submit, or propose the implementation of evidence. The fact that the law enforcement authority did not seek or request it is not grounds for the rejection of such evidence.

(3) Evidence obtained by unlawful coercion or threat of coercion may not be used in the proceedings except when used as evidence against the person that used coercion or threatened coercion.

Experts

Invitation of Experts

Section 105

(1) If the clarification of the facts relevant to the criminal proceedings requires the necessary expertise, the law enforcement authority will request a professional opinion. If such a procedure is not sufficient due to the complexity of the assessed issue, an expert is invited by the law enforcement authority. In the preliminary hearings, an expert is invited by the law enforcement authority which considers an expert opinion to be necessary for the

decision if the matter was referred back for further investigation by the public prosecutor and, in proceedings before the court, the presiding judge. The accused and, in proceedings before the court, the public prosecutor, shall be notified on the invitation of an expert. Another person is notified on the invitation of an expert if it is necessary for such a person to perform or tolerate something for the purpose of the expert opinion.

(2) In selecting a person who is to be invited as an expert, it is important to take the reasons for which the expert is excluded from the presentation of an expert opinion under the special Act into account. In seeking a professional opinion, the law enforcement authority shall consider whether the person from whom the professional opinion is requested is not biased in regard to their relationship to the accused, other persons involved in the criminal proceedings, or their relationship to the case.

(3) Objections against the expert may be raised on grounds set out by the special Act. In addition, objections can be raised against the professional interests of an expert or on the wording of the questions given to the expert. In the preliminary hearings, the merits of such objections shall be judged by the public prosecutor and, in proceedings before the court, the presiding judge before whom the proceeding is being conducted during the time of the objections' notification; if the objections are raised by appeal they shall be reviewed by the authority competent to decide on the appeal. If the authority grants the objections and the reasons for requesting an expert opinion still exist, they will take steps to either request an expert opinion by another expert or by re-phrasing the questions; conversely they shall instruct the person who raised the objection that no reasons for the objection were found. The opinion to the objections raised in an appeal normally forms part of the justification of the decision of the appeal.

(4) If it is particularly important to clarify the facts, it is necessary to invite two experts. Two experts must be invited if it regards an examination or an autopsy of a corpse (Section 115). The physician who treated the deceased for a disease, which immediately preceded the death, may not be invited as an expert.

(5) Pursuant to Subsection 1, even a person who is, under special Act, registered in the registry of experts and a natural person and legal entity that

has the required professional expertise may be asked for their professional opinion. The public authority shall always submit the professional opinion to the law enforcement authorities free of charge.

Section 106

An expert must be instructed on the consequences of the failure to appear on summons (Section 66) and the obligation to report the facts for which they could be excluded or could otherwise prevent them to be active in the matter as an expert without undue delay. The expert must also be instructed about the importance of the expert opinion in terms of general interest and the criminal consequences of perjury and a knowingly false expert opinion; this also applies to an expert who submitted an opinion on the basis of a request of a party pursuant to Section 89 Subsection 2.

Section 107

Preparation of Opinion

(1) An expert who is responsible for an act shall be provided with the necessary explanations from the files, and their functions should be defined. At the same time, it is therefore important that the expert does not evaluate the evidence and solve any legal issues. If it is necessary for the submission of the opinion, the experts are allowed to view the files or the files are loaned to them. They may also be allowed to be present during the interrogation of the accused and the witnesses to ask them questions related to the subject matter of the expert investigation. In justified cases, experts will be permitted to take part in another act of the criminal proceedings, provided such an act is important for the expert opinion. The expert may also suggest that other evidence is first needed to clarify the circumstances necessary for the submission of the opinion.

(2) An expert invited along to submit an expert opinion on the cause of death or the deceased person's medical condition is entitled to require medical documentation concerning such persons; in other cases they may require medical documentation under the conditions provided by the special Act.

(3) Experts are usually requested to prepare a written version of the expert opinion. The expert opinion is also served to the defence counsel at the expense of the defence.

Section 108

Interrogation of an Expert

(1) If an expert has prepared a written expert opinion, it is enough to refer to it and confirm it during the interrogation. If the opinion was not prepared in writing, the expert shall dictate it for the transcript during the interrogation.

(2) If several experts were invited who, after a mutual consultation, arrived to affirmative conclusions, the expert opinion shall be submitted by an expert appointed to do so by the others; if their opinions are different, each expert must be heard separately.

(3) In the preliminary hearing, the expert opinion may be omitted if the police authority or the public prosecutor does not doubt the reliability and completeness of the submitted written expert opinion.

Section 109

Errors of Opinion

If there are doubts about the correctness of the opinion, or if the opinion is unclear or incomplete, it is necessary to ask an expert to explain. If that bears no results, another expert is invited along.

Section 110

Opinions from an Institute

(1) In exceptional cases, particularly in difficult cases requiring special scientific assessments, the police authority or the public prosecutor and, in proceedings before the court, the presiding judge may invite a public authority, scientific institute, university or a specialised institution to provide expert services to submit an expert opinion or an examination of an opinion filed by an expert.

(2) A person who was invited to provide an expert opinion or to examine an opinion filed by an expert under Subsection 1 shall provide a written opinion. It will include the identification of the person or persons who prepared the opinion and if necessary, they may be heard as an expert; if it was necessary to invite two experts (Section 105 Subsection 4), they will list at least two such persons.

(3) In selecting persons referred to in Subsection 2 it is important to take the reasons for which the expert is excluded from submitting the expert opinion under special Act into account.

(4) The provisions of Section 105 Subsection 3 are similarly applicable when requesting the opinion from an institute.

Section 110a

If the expert opinion submitted by a party has all the elements required by law and includes an expert clause that they are aware of the consequences of giving a knowingly false expert opinion, then the performance of such evidence is the same as if it was an expert opinion requested by a law enforcement authority. The law enforcement authority shall allow the experts that were requested for an expert opinion by one of the parties to inspect the file, or will otherwise allow them to become familiar with the information necessary for the preparation of the expert opinion.

Section 111

Use of Special Regulations on Experts

(1) Special regulations apply to the provisions of an expert, their eligibility for this function, and their exclusion from it, on the right to deny the performance of an expert act, and on the oath and reminder of the responsibilities prior to the performance of the expert act, as well as the reimbursement of cash expenses and remuneration (expert fees) for the expert act.

(2) The amount of expert fees is determined by those who invited the expert and, in proceedings before the court, by the presiding judge without undue delay or within two months of invoicing the expert fees. If those who invited the expert disagree with the amount of expert fees, then they shall decide on it by a resolution. A complaint against the resolution with a suspensive effect is permissible.

(3) The expert fees must be paid without undue delay within 30 days after they were granted.

Section 113

Purpose of the Examination and its Transcript

(1) The examination is held provided there are facts relevant to the criminal proceedings that are to be clarified by direct observation. An expert is usually invited for the examination.

(2) The examination transcript must provide a full and fair picture of the examination subject; therefore photographs, drawings and other aids are to be attached to it.

Section 158

(1) The Police Authority is obliged, based on their own findings, criminal reports, and instigations by other persons and authorities on the basis of which conclusions may be made on the suspicion of a criminal offence, to take all necessary investigations and measures to reveal the facts indicating that the criminal offence was committed and directed towards identifying the offender; they are obligated to take the necessary measures to prevent the criminal activity. The appointed authorities of the Prison Service of the Czech Republic shall inform the General Inspection of Security Forces without undue delay after they initiate such investigation.

(2) 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 for knowingly false statements and if the reporting person requests it, to inform them on the effective measures taken within one month of the notification.

Section 158d

Surveillance of Persons and Items

(1) The surveillance of persons and items (hereinafter referred to as "surveillance") means acquiring knowledge about persons and items performed in a classified manner by technical or other means. If the police authority finds during the surveillance that the accused communicates with their defence counsel, they are required to immediately destroy the records with the content of the communication, and the information that they learned in this context they are not allowed to use in any way.

(2) Surveillance during which audio, video or other records are to be obtained may be performed only upon the written authorisation of the public prosecutor.

(3) If the surveillance is to interfere with in the inviolability of residence, the confidentiality of correspondence, or finding the contents of other documents and records kept in private with the use of technology, then it may be performed only with the prior authorisation of a judge. When entering a residence, no actions other than those that lead to the planting of technical equipment can be performed.

(4) The authorisation referred to in Subsection 2 and 3 can only be issued upon written request. The request must be justified by a suspicion of specific criminal activity and, if known, with the information about the persons or items that are to be surveilled. The authorisation must state the period during which the surveillance will be carried out and this must not be longer than six months. This period may be extended by those who authorised it on the basis of a new written request, but still not exceeding six months.

(5) If the matter cannot be delayed and it is not a case referred to in Subsection 3, the surveillance may be initiated even without prior authorisation. However, the police authority is obliged to additionally request the authorisation without undue delay and if it is not received within 48 hours they are required to cease the surveillance, destroy any records, and not to use any information found in this context.

(6) Without compliance with the conditions referred to in Subsection 2 and 3, the surveillance may performed only if the person whose rights and freedoms are to be interfered with by surveillance gives their express consent. If such consent is subsequently withdrawn, surveillance shall immediately terminate.

(7) If the record of the surveillance is to be used as evidence, it is required that the transcript is attached with the particulars referred to in Section 55 and 55a.

(8) If no facts important to the criminal proceedings were found, it is necessary to destroy the records in the prescribed manner.

(9) Operators of telecommunications activity, their employees, and other persons who participate in the operation of telecommunications activity, as well as the post office or the person performing the transport of the consignments are obligated to provide the police authority performing the surveillance with the necessary assistance free of charge and in accordance with their instructions. At the same time, they may not claim the obligation of professional confidentiality imposed by special Acts.

(10) In a criminal matter other than that which the surveillance was performed for under the conditions referred to in Subsection 2, the records obtained through surveillance and the attached transcript may be used as evidence only if there is, in this case, a pending criminal proceeding on an intentional criminal offence or if the person whose rights and freedoms the surveillance interfered with, gives their consent.

Section 314l

(1) Upon the petition of the person referred to in Section 88 Subsection 8, the Supreme Court, in closed hearing, shall examine the legality of the warrant for the interception and recording of the telecommunications service.

(2) Upon the petition of the person referred to in Section 88a Subsection 2, the Supreme Court, in closed hearing, shall examine the legality of the order for the ascertainment of data on the telecommunications service.

Section 314m

(1) If the Supreme Court finds that the warrant for the interception and recording of the telecommunications service or the order for the ascertainment of data on the telecommunications service was issued or its performance was contrary to law, they shall pronounce the violation of the law by a resolution.

(2) An appeal against such decision is not permissible.

Section 314n

(1) If the Supreme Court finds that the warrant for the interception and recording of the telecommunications service was issued and its performance was in compliance with the conditions set out in Section 88 Subsection 1 or the order for the ascertainment of data on the telecommunications

service was issued and its performance was in compliance with the conditions set out in Section 88a Subsection 1, they shall pronounce in a resolution that the law was not violated.

(2) An appeal against such decision is not permissible.

Act No. 104/2013 Sb., on international judicial cooperation in criminal matters[5]

Section 64

Cross-border Interception of Communications

(1) If an international treaty stipulates that it is possible to perform interception of telecommunications in from a foreign state the territory of the Czech Republic without its technical assistance, the competent authority to decide on granting the authorization to performing the interception or with proceeding therewith and to related actions will be the Regional Court in Prague; if there is pre-trial proceeding being conducted in the state performing the interception, the Regional Court in Prague will decide upon a petition of a public prosecutor of the Regional Public Prosecutor's Office in Prague. The authorization to perform the interception or to proceed therewith may be granted only if the conditions of Section 88 of the Code of Criminal Procedure are met.

(2) If an international treaty stipulates that interception of communications may be performed in the territory of the Czech Republic without its technical assistance, the public prosecutor and after lodging an indictment the judge will inform the foreign state in a manner provided for by the international treaty of the anticipated or conducted interception.

5 Informal translation made by the authors.

Act No. 127/2005 Sb., on electronic communication and on amendment to some related laws (Electronic Communications Act)[6]

Section 2

Definitions

For the purposes of this Act

[…]

f) "provision of an electronic communications network" means the establishment, operation or supervision of such a network, or making it accessible,

[…]

h) "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other facilities, including network elements which are inactive and which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed circuit-switched or packet-switched networks and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting and cable television networks, irrespective of the type of information conveyed,

[…]

j) "public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services, and which supports the transfer of information between network termination points, or an electronic communications network through which a service distributing radio and television broadcasts is provided,

[…]

n) "electronic communications services" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting,

6 Informal English translation available online at http://www.mpo.cz/dokument156553.html

and on cable television networks, but excluding services that offer content by means of electronic communications networks and services, or exercise editorial control over the offered content transmitted using electronic communications networks and services; it does not include information society services, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks,

o) "publicly available electronic communications service" means an electronic communications service from the use of which no person is excluded beforehand,

[…]

Section 87

(1) The rights and obligations relating to personal data protection, not regulated in this Volume, shall be governed by a special legal regulation.

(2) For the purposes of this Volume, consent based on a special legal regulation shall also be understood to mean consent granted by electronic means, including, but not limited to, the completion of an electronic form on the Internet.

(3) Supervision over compliance with obligations while processing personal data according to this Act shall be provided by the Office for Personal Data Protection in accordance with a special legal regulation.

Section 88

Securing the Protection of Personal, Traffic and Location Data and the Confidentiality of Communications

(1) An undertaking providing a publicly available electronic communications service is obliged to:

a) take technical and organisational measures to safeguard the security of the service in respect of the protection of natural persons' personal information in accordance with a special legal regulation, protection of traffic and location data, and confidentiality of the communications of natural persons and legal entities in providing the service; if necessary, the provider concerned shall, upon written agreement, also cooperate with the undertaking providing the communications network to provide protection,

b) prepare internal technical and organisational regulations to provide data protection and communications confidentiality in accordance with Clause (a) above; secure data protection and communications confidentiality with respect to the existing technical capabilities and the costs needed to provide protection at a level adequate to the risks of compromising the protection,

c) inform the subscribers concerned about the specific risk of the disturbance of network security in relation to data protection in accordance with Clause (a) above, and if the risk is beyond the scope of the measures taken by the undertaking, it shall also inform the subscribers about all the possible ways of remedying the situation, including the costs associated therewith,

d) establish internal procedures for handling requests for access to users' personal data; at the request of the Office for Personal Data Protection, undertakings providing a publicly available electronic communications service shall provide it with information about these procedures, the number of applications received, the legal justification of such requests and their responses.

(2) An undertaking providing a publicly available electronic communications service shall submit to the Office, if the Office so requests, the regulations referred to in Subsection 1 (c). If the Office finds that those regulations are in contradiction with this Act, the Office shall immediately notify the undertaking to that effect and shall grant the undertaking a reasonable period of time to remove any deficiencies.

(3) The Office is entitled, having requested the submission of the regulations referred to in Subsection 1 (b), to inspect how the undertakings providing a publicly available electronic communications service comply with those regulations, with the exception of inspections of compliance with obligations relating to the protection of personal data.

(4) In the event of a breach of protection of the personal data of a natural person, the undertaking providing a publicly available electronic communications service shall notify this fact to the Office for Personal Data Protection without undue delay. Such a notification shall contain a description of the consequences of the breach of protection and the technical protection measures the undertaking has adopted, or proposes adopting.

(5) In the event of a breach of protection of the personal data of a user pursuant to Subsection 4 might have a particularly serious impact on the privacy of a natural person, or if an undertaking providing a publicly available electronic communications service failed to take measures to remedy this situation and which would have been sufficient to protect the personal data at risk, in accordance with an assessment by the Office for Personal Data Protection, it shall also notify this fact to the individual concerned and to the Office for Personal Data Protection. In this notification, the undertaking shall indicate the nature of the breach of personal data protection, recommendations for the implementation of interventions to mitigate the impact of the breach of personal data protection and the contact information location.

(6) The Office for Personal Data Protection is entitled, after investigating the situation resulting from the breach of protection pursuant to Subsection 4 above, to impose an obligation on an undertaking providing a publicly available electronic communications service to inform the individual concerned of the breach of personal data protection, if it has not already done so.

(7) An undertaking providing a publicly available electronic communications service shall maintain, only for the purposes of reviewing compliance with obligations pursuant to Subsections 4 and 5, a list of breaches of personal data protection, including information on the circumstances of the breach, its impacts and measures adopted to remedy the situation. An implementing legal regulation may lay down more detailed conditions under which the undertaking providing a publicly available electronic communications service is required to notify any breach of personal data protection, the format of such a notification and the manner in which the notification is to be made.

Section 88a

(1) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service shall ensure that the traffic and location data stored in accordance with Section 97 Subsection 3 are of the same quality and subject to the same security and protection against unauthorised access, alteration, destruction, loss

or theft or other unauthorised processing or use, as the information referred to in Section 88; this does not affect the obligations set out in a special legal regulation34).

(2) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service shall draft internal technical and organisational rules to ensure data protection in accordance with Subsection 1; it shall provide data protection with regard to the existing technical possibilities and to the costs required to provide protection at a level appropriate to the risk of breach of protection. The provisions of Section 88 Subsections 2 to 7 shall apply mutatis mutandis to data protection under this provision

Section 89

Confidentiality of Communication

(1) Undertakings providing a public communications network or a publicly available electronic communications service shall implement technical and organisational measures to safeguard the confidentiality of the messages and the related traffic and location data, which are transmitted via their public communications network and the publicly available electronic communications services. In particular, such undertakings shall not admit any tapping, message storage, or any other types of interception or monitoring of messages, including the data contained therein and related thereto, by any persons other than the users, without the consent of the users concerned, unless otherwise provided in an Act36). This shall not be to the prejudice of the technical storage of data as needed for message transmission without affecting the confidentiality principle.

(2) A message means any information being exchanged or transmitted between a finite number of subscribers or users via the publicly available electronic communications service, except for the information transmitted as part of the public radio or television broadcasting service via the electronic communications network, unless it can be allocated to an identifiable subscriber or user receiving that information.

(3) Anybody wishing to use, or using, the electronic communications network for the storage of data or for gaining access to the data stored in the

subscribers' or users' terminal equipment shall inform those subscribers or users beforehand in a provable manner about the extent and purpose of processing such data and shall offer them the option to refuse such processing. This obligation does not apply to activities relating to technical storage or access and serving exclusively for the purposes of performing or facilitating message transmission via the electronic communications network, nor does it apply to cases where such technical storage or access activities are needed for the provision of an information society service explicitly requested by the subscriber or user.

Section 90

Traffic Data

(1) Traffic data mean any data processed for the purposes of the transmission of a message via the electronic communications network or for the billing thereof.

(2) An undertaking providing a public communications network or a publicly available electronic communications service who processes and stores traffic data, including the appropriate location data relating to a user or subscriber, shall erase such data, or render them anonymous, once they are no longer needed for message transmission, except as provided in Subsections 3 to 6. The obligation of the legal entity or natural person providing a public communications network or a publicly available electronic communications service to maintain traffic and location data in accordance with Section 97 shall remain unaffected.

(3) An undertaking providing a public communications network or publicly available electronic communications service shall store traffic data for services provided to a subscriber or user until such time as a dispute pursuant to Section 129 Subsection 3 has been resolved, or until the end of the period during which the prices may be billed or the provision of an electronic communications service may be legally challenged or settlement recovered.

(4) An undertaking providing a public communications network or a publicly available electronic communications service may process the traffic data essential for the billing of the service provided to a subscriber or user for access, to the end of the period during which payment may be recovered.

(5) Undertakings providing a public communications network or a publicly available electronic communications service may provide each other with data related to the provision of the service, including, but not limited to, data about the subscribers being connected, in order to ensure interconnection and access to the network, mutual billing, and identification of any abuse of the electronic communications network and services. Abuse of electronic communications networks and services means consistent late payment of bills in accordance with Section 64, or the making of malicious or annoying calls.

(6) For the purposes of marketing the electronic communications services, or for the provision of value-added services, the undertaking providing a publicly available electronic communications service may only process the data referred to in Subsection 1 above to the extend and for the period needed for such services or such marketing, provided the subscriber or user to whom the data relate have given their consent thereto. The subscriber or user may withdraw their consent to the processing of traffic data at any time.

(7) A value-added service means any service for which it is necessary to process traffic data – or location data other than traffic – beyond what is needed for the transmission of a message or for the billing thereof.

(8) The undertaking providing a publicly available communications service shall inform the concerned subscriber or user about the traffic data being processed and about the time for which such data may be processed for the purposes referred to in Subsections 3 to 5. For the purposes referred to in Subsection 6, the undertaking shall so inform the subscriber or user to whom the data apply before obtaining the consent of such a subscriber or user.

(9) An undertaking providing a public communications network and an undertaking providing a publicly available electronic communications service shall ensure that the traffic data processing, in accordance with Subsections 2 to 6 is restricted to:

a) the persons who were authorised to that effect by the undertaking and who are responsible for the billing or operations management, customer inquiries, fraud identification, electronic communications services marketing, or who provide value-added services, and

b) the extent essential for the activities referred to in Clause (a) above.

Section 91

Location Data

(1) Location data means any data that are processed within the electronic communications network and that define the geographical location of the terminal equipment of a user of a publicly available electronic communications service.

(2) If an undertaking providing a public communications network or publicly available electronic communications service performs the processing of location data other than traffic data, which have a bearing on a user or subscriber, such an undertaking shall render this data anonymous or obtain the user's or subscriber's consent to the processing of such data to the extent and for the period as needed for the provision of value-added services. Before gaining such consent, the undertaking shall inform the user or subscriber concerned about the type of location data to be processed other than traffic data, about the purpose and length of the processing and of whether the data are to be made available to a third party for the provision of value-added services. The user and subscriber may withdraw his/her consent to the data processing at any time.

(3) If the user or subscriber gave his/her consent to the processing of location data other than traffic data, the undertaking providing a public communications network or a publicly available electronic communications service shall offer the user or subscriber the operation of temporarily refusing the processing of the data in accordance with Subsection 2 above for every connection to the network of for every message transfer. Such an option shall be provided free of charge and only entail simple processes.

(4) An undertaking providing a public communications network, an undertaking providing a publicly available electronic communications service and an undertaking providing value-added services shall ensure that the

data referred to in Subsections 2 and 3 are only processed by persons duly authorised and entitled to that effect by internal technical and organisational regulations within the meaning of Section 88 Subsection 1 (b); the processing must be restricted to the extent essential for the needs of such activities.

Section 92

Display of Incoming Call Number

(1) An undertaking providing a publicly available telephone service is obliged, in the event that the opportunity is offered, to display the subscriber number:

a) of the calling subscriber, to offer the calling subscriber the possibility free of charge to prevent the display of his/her subscriber number for each individual call, using simple means. The calling subscriber shall have this option for each subscriber number,

b) of the calling subscriber, to offer the called subscriber the possibility of preventing the display of the calling subscriber number for incoming calls, using simple means and providing this function free of charge in justified cases, such justified cases being, without limitation, workstations from which personal crisis situations are solved (for example hot line services),

c) of the calling subscriber, and displaying this number before the call is actually connected, to offer the called subscriber the possibility of refusing the incoming calls, for which the calling subscriber restricted the display of his/her subscriber number, using simple means,

d) of the called subscriber, to offer the called subscriber the possibility of preventing the display of his/her subscriber number for the calling subscriber, using simple means and providing the service free of charge.

(2) The provisions of Subsection 1 (a) shall also apply to calls from the Member States of the European Union routed to third states. The provisions of Subsection 1 (b), (c) and (d) also apply to incoming calls from third states.

(3) Where display of the calling or called number is offered, the undertaking providing a publicly available electronic communications service shall inform the public of the possibilities referred to in Subsection 1 above.

(4) An undertaking providing a public communications network or a publicly available electronic communications service is entitled to cancel the barring of the display of the calling subscriber number:

a) temporarily, at the request of a subscriber, who has requested that a malicious or annoying call be traced; in such a case, the undertaking shall store and make accessible to the aggrieved subscriber information containing the calling subscriber identification, and

b) and continue to process the location data during the transmission of calls to every emergency call number operated by the relevant facility for the reception of such calls, even despite a temporary ban or the lack of consent from the subscriber concerned.

(5) An undertaking providing a public communications network or a publicly available electronic communications service shall make public in its commercial facilities, and in a manner allowing remote access, the mandatory procedures to be followed in order to impose the two options referred to in Subsection 4 above, and shall inform its subscribers to that effect.

Section 93

Abuse of Electronic Mail Addresses of the Sender

It is prohibited to use any electronic mail address to send a message or messages to third parties without the consent of the holder of that electronic mail address.

Section 94

Call Forwarding

(1) Any undertaking providing a public communications network or a publicly available electronic communications service shall ensure, using simple means, that every subscriber can enjoy, free of charge, the possibility of preventing automatic forwarding of calls by a third party to the subscriber's terminal equipment.

(2) In the event that, during the provision of the publicly available electronic communications service, calls are forwarded automatically or in a concealed manner to another service or to a service provided by another undertaking, or a new connection is established, thereby increasing the price

to be charged, the person providing the publicly available electronic communications service shall notify the user of this fact free of charge and allow him/her to stop the call before it is forwarded or a new call is established. If calls are forwarded or a new connection is established and, as a result, the price to be charged is increased without notification of the user to that effect by the person providing a publicly available electronic communications service at the increased price, the Office shall decide to stop the provision of such service.

Section 95

Subscriber Directories

(1) Anybody gathering subscribers' personal data in order to issue a subscriber directory, whose purpose is to search for detailed contact information about persons on the basis of their names and, if applicable, other identifying elements, to the minimum extent necessary, shall:

a) inform the subscribers concerned, free of charge and before the inclusion of their data in the directory, of the purpose of the printed of electronic directory of subscribers, which is to be made available to the public either directly or through the subscriber directory inquiry services, as well as of other possibilities for its use, based on the search functions contained in the electronic versions of the directory,

b) obtain the prior consent of the subscribers to the publication of their personal data in accordance with Section 41 Subsection 5 and ensure that the subscribers have an opportunity to determine which of their personal data, from the range of information relevant for the purposes of the directory, as defined by the directory publisher, are to be included in the public directory; further, it must be ensured that the subscribers are able to verify such information and to request the amendment or removal of such information. At the same time, the person gathering such information must ensure that the subscribers can indicate, with their personal information, that they do not wish to be contacted for marketing purposes. Non-inclusion in the public directory of subscribers, the verifications, corrections and removal of information from the directory and the information concerning the subscriber's wish not to be contacted for marketing purposes shall be free of charge.

(2) If the purpose of the public directory is other than to search for detailed contact information about a person on the basis of his/her name, and, if applicable, other identifying elements, to the minimum extent necessary, anybody intending to issue such a subscriber directory must first ask for the additional consent of the subscribers concerned.

Section 96

(1) It is prohibited to use electronic communications networks or services to offer any marketing advertising or any other method of offering goods or services to those subscribers who indicated in the public directory of subscribers in accordance with Section 95 Subsection 1 (b) or Section 95 Subsection 2 that they do not wish to be contacted for marketing purposes.

(2) It is prohibited to use electronic communications networks or services for the purposes of direct marketing by means of automated calling systems without human intervention (automatic calling equipment), facsimile machines or electronic mail, without the prior consent of the subscriber or user concerned.

(3) No undertaking providing subscriber directory enquiry services with information about subscriber numbers or other details may disclose any subscriber data not contained in the public directory.

(4) The provisions of Sections 95 and 96 shall apply mutatis mutandis to the data of subscribers who are legal entities.

(5) A provider of a publicly available electronic communications service, whose business interests are harmed by violations of the obligations set out in Subsections 1 to 4 above, is entitled to seek judicial protection on behalf of subscribers whose rights have been harmed by such behaviour. This does not affect the right of a party to pursue their claims in court in their own right.

Section 97

Interface for communication interception and message recording

(1) A legal entity or natural person providing a public communications network or a publicly available electronic communications service shall, at the

expense of the requesting party, provide and secure interfaces at specified points of the network to connect terminal equipment for message tapping and recording:

a) for the Police of the Czech Republic for the purposes specified in a special legal regulation,

b) for the Security Information Service for the purposes specified in a special legal regulation,

c) for the Military Intelligence service for the purposes specified in a special legal regulation.

(2) The bodies listed in Subsection 1 above shall prove their authorisation for message tapping and recording by submitting a written application, which contains a reference number under which the court ruling is filed by this body, and which is signed by the person responsible from the body listed in Subsection 1 above for the performance of the message tapping and recording. In the event of message tapping and recording by the Police of the Czech Republic in accordance with special legal regulations36) the written application shall contain a reference number under which the consent of the user of the station monitored is filed by the Police of the Czech Republic.

(3) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service shall for a period of 6 months traffic and location data which are created or processed during the operation of their public communications networks and during the provision of their publicly available electronic communications services. A legal entity or a natural person providing a public communications network or a publicly available electronic communications service is only required to store data relating to unsuccessful call attempts only when these data are created or processed and at the same time stored or recorded. At the same time, such a legal entity or natural person is required to ensure that, during the performance of the obligation referred to in the first and second sentences, no message content has been stored, and that no content

thus stored has been further distributed. A legal entity or a natural person who stores traffic and location data is required, on request, immediately to provide them to:

a) criminal law enforcement authorities for the purposes of and under the conditions laid down in a special legal regulation,

b) the Police of the Czech Republic for the purposes of initiating a search for a specific wanted or missing person, for the identification of persons of unknown identity or the identity of a corpse that has been discovered, for the prevention or detection of specific terrorist threats or for the verification of a protected person, while complying with the conditions set out in a special legal regulation,

c) the Security Information Service, for the purposes of and under the conditions laid down in a special legal regulation,

d) the Military Intelligence service for the purposes of and under the conditions laid down in a special legal regulation,

e) the Czech National Bank for the purposes of and under the conditions laid down in a special legal regulation.

After expiry of the period referred to in the first sentence above, the legal entity or natural person who stores the traffic and location data is required to destroy them, unless they were provided to the bodies authorised to use them under a special legal regulation, or unless otherwise provided in this Act (Section 90).

(4) The traffic and location data pursuant to Subsection 3 above are primarily data leading to the tracing and identification of the source and address of the communication, and also data leading to the identification of the date, time, method and duration of the communication. The scope of the traffic and location data stored in accordance with Subsection 3 above, the form and method of their transmission to the bodies authorised to use them under a special legal regulation, and the method of their disposal is stipulated in an implementing legal regulation.

(5) A legal entity or natural person providing a publicly available telephone service is required, on request, to provide information from the database of all its subscribers to the publicly available telephone service to a body

authorised to request them in accordance with a special legal regulation, at their own expense. The form and scope of the information provided is stipulated in an implementing legal regulation.

(6) Where a legal entity or natural person providing a public communications network or a publicly available electronic communications service introduces into its activities any coding, compression, encryption or any other method of transmission that makes the messages being transmitted incomprehensible, such a person shall ensure that the messages requested and the traffic and location data related thereto are provided in a comprehensible manner at the termination points for connection of the terminal equipment referred to in Subsection 1 above.

(7) For fulfilling the obligations specified in Subsections 1, 3 and 5 above, the legal entity or natural person is entitled to reimbursement for effectively incurred costs from the authorised body which requested or ordered such an action. The amount and method of reimbursement for the effectively incurred costs is set out in an implementing legal regulation.

(8) A person referred to in Subsection 1 above and its employees are required to maintain the confidentiality of any tapping or recording of messages requested or implemented in accordance with Subsections 1 and 2 and data requested or provided in accordance with Subsections 3 and 5 and matters related thereto.

(9) The technical and operational conditions and points for the connection of terminal telecommunications equipment for the tapping or recording of messages is set out in an implementing legal regulation.

(10) A legal entity or natural person providing a public communications network or a publicly available electronic communications service shall keep records on:

a) the number of cases where, on requested, it provided traffic and location data to the bodies authorised to request them,

b) the period that elapsed, in each case, from the date on which the storage of the traffic and location data began to the date on which the authorised body requested such data, and

c) the number of cases when it was not able to comply with a request to provide traffic and location data.

(11) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service is required to provide to the Office the collective records referred to in Subsection 10 above, for the previous calendar, in electronic form, at the latest by 31 January of the following calendar year. The records provided may not contain personal and identification data. The Office shall immediately send the collective records received to the Commission.

(12) The form of the records provided under Subsection 11 and the method of their submission to the Office is stipulated in an implementing legal regulation.

Section 98

The Security and Integrity of Public Electronic Communications Networks and Services

(1) An undertaking providing a public communications network or a publicly available electronic communications service shall ensure the security and integrity of its network and the security of the services it provides. For this purpose, the undertaking is, in particular, entitles to adopt technical and organisational rules created in accordance with network plans pursuant to Subsection 2. With regard to the technical capabilities of these rules to ensure a level of security that corresponds to the existing level of risk, with the aim of preventing or minimising the impact of incidents on users and of the interconnection of networks. Security of networks and services means their ability to resist random incidents or unlawful or malicious actions that seriously compromise the availability or interoperability of services and network integrity.

(2) To ensure the integrity of public communications networks, the Office shall issue network plans (Section 62), in which it defines the basic characteristics of those networks and their interfaces which are essential for the interconnection of public communications networks, for access thereto, for the connection of non-public communications networks and to ensure the continuity of provision of those services which are provided through public communications services.

(3) An undertaking providing a public electronic communications network or a publicly available electronic communications service may adopt a measure to suspend provision of the service or to deny access to the service in cases where there is a threat or occurrence of a serious breach of the security and integrity or its network as a result of damage or destruction of electronic communications facilities, mainly due to major industrial accidents or natural disasters. Such suspension or denial of service must be restricted to the time strictly necessary and, if it is technically possible, access to emergency numbers must be maintained.

(4) An undertaking providing a public electronic communications network or a publicly available electronic communications service shall immediately inform the Office, the entities operating facilities for reception of emergency calls – and, using suitable means, also the users – about the serious breach to security and the loss of network integrity, the extent and reasons for the suspension of the services provided or the denial of access thereto, the measures adopted and of the expected time of removal of the causes pursuant to Subsection 3. The scope and form of the information to be provided shall be stipulated by the Office in an implementing legal regulation. In the event that this information is published in the public interest, the Office may inform the general public thereof in a suitable manner.

(5) Each year the Office shall submit to the Commission and the European Network and Information Security Agency (ENISA) a summary report for the previous calendar year, informing of the notifications and actions taken pursuant to Subsections 3 and 4, in the scope and format specified by the Commission.

(6) The Office may impose an obligation to carry out a safety audit on an undertaking providing a public communications network or a publicly available electronic communications service. This audit must be conducted by a qualified independent entity and the costs shall be borne by the undertaking. An undertaking providing a public communications network or a publicly available electronic communications service is also required, at the request of the Office, to submit to it the information needed to assess network security and integrity and service security, the safety audit and the results thereof.

Section 99

Security, Integrity and Service Provision in Crisis Situations

(1) In a crisis situation, an undertaking providing a public communications network or a publicly available electronic communications service is required, following its own technical and organisational rules, to ensure the security and integrity of its network and the interoperability of the services provided. The particulars to be included in the technical and organisational rules are stipulated by the Office in an implementing legal regulation.

(2) An undertaking referred to in Subsection 1 above shall submit to the Office at its request documents specifying the technical and organisational rules referred to in Subsection 1 above and shall allow the Office to monitor compliance with these rules. In the event any discrepancy is found between these documents and the legal regulations, the Office is entitled to inform the undertaking concerned of this fact and to set it a reasonable period within which such discrepancies are to be removed.

(3) An undertaking providing a public communications network or a publicly available telephone service is entitled, when a crisis situation is threatened or during a crisis situation39), at the request of the Ministry of Interior, to provide priority connections to the public communications network and access to the publicly available telephone service to crisis communications subscribers, in accordance with a special legal regulation. For that purpose, it is entitled, to the extent to which it is absolutely necessary, to restrict or suspend the provision of a publicly available telephone service. It shall immediately inform the Office of any restriction or suspension of a publicly available telephone service, including the scope thereof. This restriction may only be imposed for the period for which it is absolutely necessary, and access to emergency numbers must be maintained.

(4) In a crisis situation, an undertaking referred to in Subsection 1 above shall immediately inform the Office of any threat to or breaches of the security and integrity of its network and the security of services, including measures adopted or envisaged to remedy this situation and the date by which the causes are expected to be removed.

Act No. 273/2008, on the Police of the Czech Republic[7]

Section 11

Adequacy of the procedure

A policeman and police employee are required to ensure that no person suffered unwarranted injury due to their actions, ensure that their decision not to act did not resulted in unsubstantiated harm to persons whose security is endangered, proceed in a way that any possible interference with the rights and freedoms of persons to whom the act is directed, or any others, did not exceed what is necessary to achieve the objective pursued by the act.

Section 19

Technical Support

(1) The police can technically provide the use of intelligence technology or bait and security technology or a surveillance of persons and goods at the request of a public authority, which is authorised for such use.

(2) The public authority in the request demonstrates that the use of intelligence technology or surveillance of people and goods is authorised under special legal act.

Section 66

Obtaining information from records and databases

(1) Police may, in cases prescribed by law and to the extent necessary to fulfil a specific task, request a legal or natural person providing a public communications network or publicly available electronic communications with the traffic and location data in a manner, which enables remote and continuous access, unless another law provides otherwise. These persons are obliged to grant the request without undue delay, as and to the extent determined by other legislation.

(2) The Police may, to the extent necessary for meeting a specific task, demand from the owner or administrator of a register or database to be provided with information, online and without any interruption, from the database of customers of publicly accessible telephone networks, the register of personal identity cards, the register of travel documents, the register

7 Informal translation provided by the Ministry of Justice.

of diplomatic and service passports, the information system of the register of inhabitants, the register of motor vehicles, the register of birth identification numbers, the register of road toll information, the land register, and the register of drivers. In the case of customers of publicly accessible telephone networks the required information shall be provided in the form and scope laid down by another legal regulation.

(3) The Police may, in cases laid down by law and to the extent necessary for meeting specific tasks, demand from a legal entity or a physical person operating a public communication network or a providing publicly accessible service of electronic communications to be provided with operational and localisation data on-line and without any interruption, unless provided otherwise by another legal regulation. The listed persons shall be obliged to submit to such demand, without undue delay, and to provide information in the form and scope laid down by another legal regulation.

(4) The Police shall demand information pursuant to paragraphs (1) through (3) only in a manner which will permit the Police to maintain identification data concerning the Police unit or a Police officer, who requested such information, and data concerning the purpose of such request, at least for five years. The owner or administrator of a register or database shall be obliged to hold information under the first sentence in confidence.

(5) For the purpose of protecting a person about whom there is reasonable grounds to suspect that his/her life or health could be endangered, or for the purpose for searching for a wanted or missed person, the Police and the Ministry may demand from the owner or administrator of the register or database, which is maintained under special legal regulations, to provide the Police with information on each provision of personal data.

Section 68

Search for persons and things

(2) Police can request legal or natural person providing a public communications network or publicly available electronic communications service traffic and location data in a manner enabling remote and continuous access, for a purpose of ongoing search for wanted or missing persons and for the purpose of identifying a person of unknown identity or the identity of the

found corpse, unless another law provides otherwise. The information is provided in the form and to the extent determined by other legislation.

Section 71

A police division, competent in fight against terrorism, may for the purpose of preventing and detecting specific threats of terrorism to the extent necessary to request the

a) legal or natural person providing a public communications network or publicly available electronic communications to provide traffic and location data in a manner enabling remote and continuous access, unless another law provides otherwise; Information will be provided in the form and to the extent determined by other legislation.

Section 78

Handover of information

(1) Police hands over information including the information processed in the police registers, which are gained during carrying out its tasks, to the national member of Eurojust, the National Security Office, the intelligence services of the Czech Republic, Military Police, the Ministry, the Prison Service of the Czech Republic, the Customs Administration of the Czech Republic and other public authorities, if it is necessary to perform the tasks within their scope.

(2) The Police does not pass the information if it would jeopardize the accomplishment of police tasks.

Section 98

Supervision of the use of interception and recording of telecommunications, use of surevillance of persons and items and interference with the operation of electronic communications

(1) Supervision of the use of interception and recording of telecommunications, use of surevillance of persons and items under other legislation, and interference with the operation of electronic communications is performed by the Chamber of Deputies, which for this purpose establishes a supervisory body. The supervisory body shall consist of MPs designated by the Chamber of Deputies.

(2) Supervision pursuant to paragraph 1 is performed by the supervisory body in the relevant police departments, after notification to the Minister. The Minister presents to the supervisory body at least twice a year a report on the use of these measures. This does not affect the right of the supervisory body to require information and participation in meetings from others.

(3) Minister shall submit to the Government, to the relevant committee of the Chamber of Deputies and to supervisory body once a year analysis of the use of measures listed in paragraph 1.

(4) The procedure in this provision is not affected by the directive on controlling.

Act No. 17/2012 Sb., on Customs service of the Czech Republic[8]

Section 4

Jurisdiction

(5) The General directorate of customs

c) in cooperation with public authorities secures, especially technically, the use of intelligence and security equipment or surveillance of persons and things, if the relevant public authority proves that the it is authorized by law to conduct the interception.

Section 57

Handover of information

(1) Customs authorities shall hand over information to

a) police,

b) intelligence services of the Czech Republic,

c) Military Police

d) Ministry of Interior,

e) Prison Service of the Czech Republic,

f) the National Security Office and

g) other public authorities, which in the area of competence of the customs administration are responsible for supervision or which conduct the proceedings on an administrative offense.

8 Informal translation made by the authors.

(2) Customs authorities hand over the information referred to in paragraph 1 only if the information is necessary for the performance of the legal tasks of these bodies.

(3) Customs authorities shall not transmit information when it would significantly jeopardize the performance of its duties

Section 63

Basic Condition of Use

(1) Bodies of Customs service may use operative search means, interception and recording of communication (thereinafter "operative search means ") as set in the Criminal Procedure Act, when fulfilling duties arising from international treaties during conducting of control of persons, about whom there exist serious reasons to suspect that they are breaching or have breached law of the second party to the treaty.

(2) Rights and duties of bodies of customs service arising from the statutes regulating criminal procedure are not affected by conduct of control in the meaning of paragraph 1.

(3) Operative search means may be used only in situation, when the breach of law of the second party to the treaty, would be considered in accordance with the Criminal code[9] as an intentional crime, should it happen in the territory of the Czech Republic.

Section 64

(1) Usage of operative search means must not follow any other purpose than the one, which is specified in the concerned international treaty. Rights and freedoms of intercepted persons can be restrained on in the necessary manner.

Act No. 341/2011 Sb., on General Inspection of Security Force[10]

Section 9

(3) General Inspection may require from Security Forces and other public authorities, if it is necessary for the performance of a specific task of the Inspection

9 Act No. 40/2009 Sb., the Criminal Code.

10 Informal translation made by the authors.

a) technical and personal resources for interception and recording of telecommunication operations or for operative intelligence means. In the request the Inspection demonstrates that the use of interception and recording of telecommunication operations or monitoring people and things have been permitted under the Criminal Procedure Code.

Section 37

Handover of information

(1) Inspection hands over information, including personal data and information processed in the records of inspection, which are gained in carrying out its tasks to the Czech Republic Police, Prison Service of the Czech Republic, the Customs Administration of the Czech Republic, the Czech Republic's intelligence services, military police and other public authorities, if it is necessary to perform the tasks within their jurisdiction.

(2) The Inspection shall without undue delay hand over information which were collected during carrying out its tasks and which can be used in course of exempting a member of security forces from a service to the Director of the security forces; If this member is the director of a national security force, the inspection passes the information to his superior, Staff officers.

(3) Inspection of the information referred to in paragraphs 1 and 2 are not handed over, if it would undermine tasks of the Inspection.

Act No. 137/2001 Sb., on special protection of a witness and other persons in connection with criminal proceedings and on change of the act No. 99/1963 Sb., Civil procedure code[11]

Section 10a

Permission to check on a protected person

(1) If there is given suspicion that the protected person fails to comply with the obligations specified in Section 6, and is unable to verify this suspicion in another way, the Police is authorised, to the strictly necessary extent, to gain knowledge in a classified manner using technical or other means. The Police is authorised to make sound, visual or other records, conduct interception of communication and require on the person performing

11 Informal translation made by the authors.

telecommunications services data on telecommunications traffic, which are the subject of telecommunications secrecy and subject to the protection of personal and agency data.

(2) Acquisition of audio, video or other recordings, interception and recording of telecommunications traffic and requesting data on telecommunications traffic is possible only with the prior consent of the presiding judge of the High Court into whose jurisdiction belongs the seat of the police department or the prison service, which provides special protection and assistance. Against a decision to authorize or reject the application is not subject to appeal.

Act No. 153/1994 Sb., on intelligence services of the Czech Republic[12]

Section 8

Reporting by Intelligence Services and tasking Intelligence Services

(3) Intelligence services report to public and police authorities information about findings, which fall within their jurisdiction. This does not apply if providing of the information threatens important interest pursued by the relevant intelligence service

Section 9

Intelligence services cooperate with each other on the basis of agreements, which are concluded with the consent of the Government.

Act No. 154/1994 Sb., on Security Information Service[13]

Section 8

Intelligence Technology

(1) Intelligence technology for the purposes of this Act means the technical facilities and equipment, especially electronic, photo-technical, chemical, physic-chemical, radio-optical, mechanical, or their files used in classified manner, if it causes interference with the fundamental rights and freedoms in a) searching, opening, examining or evaluating transported consignments,

12 Informal translation made by the authors.
13 Informal translation made by the authors.

b) interception or recording of telecommunications, radio communication or other similar operation, or surveying data about this operation,

c) making video, audio or other records,

d) Search using technical means that could prevent or impede the fulfilment of operations within the scope of Military Intelligence/ Security Information Service,

e) identification of persons or objects, or to identify their movements using surveillance techniques and baits.

(2) Using intelligence technology, if it is not interfering with fundamental rights and freedoms, is not

a) capturing, listening, monitoring and evaluating information, which are distributed in a way that allows to access them by previously undefined group of persons

b) making video or audio recordings,

c) use security techniques and baits,

d) monitoring of telecommunications, radio communication or other similar operations without tapping its content, or collecting data on the traffic.

Section 8a

The Security Information Service is entitled to the extent required for the performance of a specific operation, request a legal or natural person providing a public communications network or publicly available electronic communications service

a) the establishment or security interface for connecting the terminal telecommunications equipment for the interception or recording messages at specified points of their network, and

b) the provision of operational and localization data, in the form and to the extent determined by special legislation.

Section 9

Application of intelligence technology

(1) Intelligence technology can be used by the Security Information Service only when initially authorised by a written permission of the presiding

judge of the High Court in whose jurisdiction falls the Security Information Service (hereinafter referred to as "judge"), under assumption that detecting and documenting of the activities for which is the technology to be used, would be ineffective or substantially more difficult or impossible, should it be done in a different way.

(2) Use of intelligence technology must not exceed the scope of the authorization of a judge under paragraph 1 and must not interfere with the rights and freedoms beyond what is strictly necessary.

(3) The Security Information Service can technically secure the use of intelligence technology for the needs of other competent authorities, if they so request and submit appropriate authorization for the use of intelligence technology issued by a special legal regulation.

(4) The Security Information Service is entitled to demand from the other for such activity authorized bodies the use of technical security intelligence technology for its own use. In this case, it is obliged to demonstrate that the use of intelligence technology has been authorised under provision this Act.

Section 10

Authorisation to the use of intelligence technology

(1) The judge will issue the authorisation to the use of intelligence technology on the basis of written request, which includes

a) kind of intelligence technology, which is going to be used, period of time during which it is going to be used, basic identification data about the person (if known), against which the technology is going to be used, number of telephone or other similar station, should it be used for the communication interception, as well as the place of use of intelligence technology. Should the intelligence technology be used against member of government, member of Parliament or judge of the Constitutional court, or should the right to untouchability of household be breached, this information must be included in the request;

b) reasons for the use of intelligence technology;

c) information about any prior use of information technology against person indicated in the letter a) including the information, how was decided about that request.

(2) The judge will decide about the request without delay.

(3) The use of intelligence technology can be authorised only for the necessary period of time, at longest for 3 months. This period of time can be prolonged after a new request, but maximally only for 3 more months.

(4) The decision about authorisation to use of intelligence service includes kind of intelligence technology, which is going to be used, period of time during which it is going to be used, basic identification data about the person (if known), against which the technology is going to be used, number of telephone or other similar station, should it be used for the communication interception, as well as the place of use of intelligence technology.

(5) The judge issues along with the decision about authorisation to use of intelligence service also an abstract made from this decision, which includes the necessary identification data and statement, whether by use of intelligence service is breached the right to untouchability of household. The abstract does not include reasoning.

(6) Should the judge deny the request for authorisation to the use of intelligence technology, the decision must contain reasoning for such decision.

(7) Appellation against the decision is not allowed.

Act No. 289/2005, on Military Intelligence[14]

Section 8

Intelligence Technology

(1) Intelligence technology for the purposes of this Act means the technical facilities and equipment, especially electronic, photo-technical, chemical, physic-chemical, radio-optical, mechanical, or their files used in classified manner, if it causes interference with the fundamental rights and freedoms in a) searching, opening, examining or evaluating transported consignments,

b) interception or recording of telecommunications, radio communication or other similar operation, or surveying data about this operation,

c) making video, audio or other records,

14 Informal translation made by the authors.

d) Search using technical means that could prevent or impede the fulfilment of operations within the scope of Military Intelligence/ Security Information Service,

e) identification of persons or objects, or to identify their movements using surveillance techniques and baits.

(2) Using intelligence technology, if it is not interfering with fundamental rights and freedoms, is not

a) capturing, listening, monitoring and evaluating information, which are distributed in a way that allows to access them by previously undefined group of persons

b) making video or audio recordings,

c) use security techniques and baits,

d) monitoring of telecommunications, radio communication or other similar operations without tapping its content, or collecting data on the traffic.

Section 9

Application of intelligence technology

(1) Intelligence technology can be used by The Military Intelligence only when initially authorised by a written permission of the presiding judge of the High Court in whose jurisdiction falls the Ministry of Defence (hereinafter referred to as "judge"), under assumption that detecting and documenting of the activities for which is the technology to be used, would be ineffective or substantially more difficult or impossible, should it be done in a different way.

(2) Use of intelligence technology must not exceed the scope of the authorization of a judge under paragraph 1 and must not interfere with the rights and freedoms beyond what is strictly necessary.

(3) The Military Intelligence can technically secure the use of intelligence technology for the needs of other competent authorities, if they so request and submit appropriate authorization for the use of intelligence technology issued by a special legal regulation.

(4) The Military Intelligence is entitled to demand from the other for such activity authorized bodies the use of technical security intelligence technology for its own use. In this case, it is obliged to demonstrate that the use of intelligence technology has been authorised under provision this Act.

(5) Military Intelligence is entitled to the extent required for the performance of a specific operation, request a legal or natural person providing a public communications network or publicly available electronic communications service

a) the establishment or security interface for connecting the terminal telecommunications equipment for the interception or recording messages at specified points of their network, and

b) the provision of operational and localization data, in the form and to the extent determined by special legislation.

Section 10

Authorisation to the use of intelligence technology

(1) The judge will issue the authorisation to the use of intelligence technology on the basis of written request, which includes

a) kind of intelligence technology, which is going to be used, period of time during which it is going to be used, basic identification data about the person (if known), against which the technology is going to be used, number of telephone or other similar station, should it be used for the communication interception, as well as the place of use of intelligence technology. Should the intelligence technology be used against member of government, member of Parliament or judge of the Constitutional court, or should the right to untouchability of household be breached, this information must be included in the request;

b) reasons for the use of intelligence technology;

c) information about any prior use of information technology against person indicated in the letter a) including the information, how was decided about that request.

(2) The judge will decide about the request without delay.

(3) The use of intelligence technology can be authorised only for the necessary period of time, at longest for 3 months. This period of time can be prolonged after a new request, but maximally only for 3 more months.

(4) The decision about authorisation to use of intelligence service includes kind of intelligence technology, which is going to be used, period of time during which it is going to be used, basic identification data about the person (if known), against which the technology is going to be used, number of telephone or other similar station, should it be used for the communication interception, as well as the place of use of intelligence technology.

(5) The judge issues along with the decision about authorisation to use of intelligence service also an abstract made from this decision, which includes the necessary identification data and statement, whether by use of intelligence service is breached the right to untouchability of household. The abstract does not include reasoning.

(6) Should the judge deny the request for authorisation to the use of intelligence technology, the decision must contain reasoning for such decision.

(7) Appellation against the decision is not allowed.

Act No. 15/1998 Sb., on the supervision in the area of capital market and change and supplementation of some acts

Section 8

(1) The Czech National Bank is entitled for the purpose of performance of supervision over capital market to a) request, after prior written authorisation by the presiding judge of the High Court under whose jurisdiction belongs the seat of the Czech National Bank, from a legal or natural person providing a public communications network or publicly available electronic communications traffic and location data in accordance to special legislation, if it can be reasonably assumed that data provided may contribute to the clarification of facts important for the detection of an administrative offense in the area of business or commerce in the capital market under the act governing capital market undertakings, including the offender, and if the pursued objective cannot be achieved differently, or if can be achieved only by exerting a disproportionate effort.

Act No. 101/2000 Sb., on personal data protection and change of some acts[15]

Section 3

(6) The provisions of Article 5(1) and Articles 11 and 12 of this Act shall not apply to processing of personal data necessary to fulfil obligations of the controller provided by special Acts to ensure:

(a) security of the Czech Republic,

(b) defence of the Czech Republic,

(c) public order and internal security,

(d) prevention, investigation, detection and prosecution of criminal offences,

(e) important economic interest of the Czech Republic or of the European Union,

(f) important financial interest of the Czech Republic or of the European Union, in particular the stability of financial market and currency, functioning of currency circulation and system of payments as well as budgetary and taxation measures, or (g) exercise of control, supervision, surveillance and regulation related to exercise of public authority in the cases under (c), (d), (e) and (f), or (h) activities related to disclosure of files of the former State Security.

Section 5

(1) The controller shall be obliged to:

(a) specify the purpose for which personal data are to be processed;

(…)

(d) collect personal data corresponding exclusively to the specified purpose and in an extent that is necessary for fulfilment of the specified purpose;

(e) preserve personal data only for a period of time that is necessary for the purpose of their processing. After expiry of this period, personal data may be preserved only for purposes of the state statistical service, and for scientific and archival purposes. When using personal data for these purposes,

15 Informal translation available at https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156 & id_ktg=1107.

it is necessary to respect the right to protection of private and personal life of the data subject from unauthorised interference and to make personal data anonymous as soon as possible;

(f) process personal data only in accordance with the purpose for which the data were collected. Personal data may be processed for some other purpose only within the limits of the provisions of Article 3(6) or if the data subject granted his consent herewith in advance;

(…)

(h) ensure that personal data that were obtained for different purposes are not grouped.

(2) The controller may process personal data only with the consent of data subject. Without such consent, the controller may process the data:

(a) if he is carrying out processing which is essential to comply with legal obligation of the controller;

(b) if the processing is essential for fulfilment of a contract to which the data subject is a contracting party or for negotiations on conclusion or alteration of a contract negotiated on the proposal of the data subject;

(c) if it is essential for the protection of vitally important interests of the data subject. In this case, the consent of data subject must be obtained without undue delay. If the consent is not granted, the controller must terminate the processing and liquidate the data;

(d) in relation to personal data that were lawfully published in accordance with special legislation. However, this shall not prejudice the right to the protection of private and personal life of the data subject, or (e) if it is essential for the protection of rights and legitimate interests of the controller, recipient or other person concerned. However, such personal data processing may not be in contradiction with the right of the data subject to protection of his private and personal life.

(f) if he provides personal data on a publicly active person, official or employee of public administration that reveals information on their public or administrative activity, their functional or working position, or (g) if the processing relates exclusively to archival purposes pursuant to a special Act.

(3) If the controller processes personal data on the basis of a special Act, he shall be obliged to respect the right to protection of private and personal life of the data subject.

Section 12

Data subject's access to information

(1) If the data subject requests information on the processing of his personal data, the controller shall be obliged to provide him with this information without undue delay.

(2) The contents of the information shall always report on:

(a) the purpose of personal data processing;

(b) the personal data or categories of personal data that are subject of processing including all available information on their source;

(c) the character of the automated processing in relation to its use for decision-making, if acts or decisions are taken on the basis of this processing the content of which is an interference with the data subject's rights and legitimate interests;

(d) the recipients or categories of recipients.

(3) For provision of this information the controller shall be entitled to require a reasonable reimbursement not exceeding the costs necessary for provision of information.

(4) The controller's obligation to provide the data subject with information pursuant to Article 12 may be met by a processor on behalf of the controller.

Act No. 412/2005 Sb. on protection of secret information and security

Section 107

Acts in the proceeding on issuance of personnel security clearance certificates

(3) In the proceedings on issuance of personnel security clearance certificates for the Top Secret degree the Office (National Security Authority)

shall conduct all the acts according to the paragraph 2 and furthermore it requests competent intelligence service to conduct an examination of possible security risks in the environment, in which the subject operates

Decree No. 336/2005 Sb. on technical and operational conditions and points of connection of the telecommunications equipment for interception and recording of telecommunications traffic

Section 7

(1) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service (hereinafter referred to as "operator") shall equip their network or service with interface for connecting devices for interception on the basis of a request from a competent authority.

(2) If the operator is developing a new network or service, significantly expanding or changing the existing network or service, they shall prompt the competent authority to issue a request for equipping the network or service with an interface for connecting interception devices. The competent authority shall issue the request within 15 days from the prompting.

(3) On the basis of request issued according to the paragraph 1 or 2, the operator in cooperation with the competent authority shall propose possible technical solutions, including the reasons for their implementation and a calculation of the cost of each solution.

(4) The chosen solution and its parameters shall be specified in a record jointly elaborated by the competent authority and the operator. The record shall also include a calculation of financial costs and the method and schedule of the payment.

Packet networks outputs

Section 13

(1) The output of the network or service is provided via

a) a hard data link, or

b) a secure virtual channel on the Internet using the standardized communication protocol FTP, server shall be provided by a competent authority and operator should connect as a client.

(2) The sent data unit shall be equipped with an identifier of user address and a serial number or a time stamp. The data integrity of the data unit shall be ensured by creating a file stamp using the hash function SHA-1.

(3) During the interception of emails, the operator may, with consent from the competent authority, send copies of messages using protocol for transferring email to the SMTP server provided by the competent authority.

INTERCEPTION OF ELECTRONIC COMMUNICATIONS IN THE CZECH REPUBLIC AND SLOVAKIA

Mgr. MgA. Jakub Míšek, Assoc. Prof. JUDr. Radim Polčák, Ph.D., Mgr. Václav Stupka, Mgr. Pavel Loutocký, BA (Hons), Mgr. Tomáš Abelovský

Published by Masaryk University, Žerotínovo nám. 617/9, 601 77 Brno
Publications of the Masaryk University No. 573
(theoretical series, edition Scientia)

Print: Point CZ, s.r.o., Milady Horákové 890/20, 602 00 Brno
1st edition, 2016

ISBN 978-80-210-8423-0

www.law.muni.cz