DATA RETENTION IN CZECH REPUBLIC: PAST, PRESENT AND FUTURE

by

MATĚJ MYŠKA*

This paper examines the legal questions related with the implementation of the electronic communications data retention in the Czech Republic as prescribed by the Directive 2006/24/EC. Firstly, the evolution of the data retention legislation, including the regulation that was in effect before the Directive is presented. As in other Member States (e.g. Romania and Germany) the implementation was challenged before the Constitutional Court and declared unconstitutional - mainly because of its vagueness. Therefore the rulings of the Constitutional court are analysed. However as stated by the Czech Constitutional Court „the subject matter of the Directive nevertheless leaves the Czech Republic enough possibilities to transpose it into the national law in conformity with the Constitution". The new "data retention reloaded" legislation is assessed whether it meets the requirement foreseen by the Constitutional Court. The paper concludes with general remarks on the further development of data retention in the Czech Republic in the context of the pending cases before the Court of Justice of the European Union dealing with the proportionality of the Directive 2006/24/EC.

KEYWORDS

Directive 2006/24/EC; privacy; data retention; data protection; Czech law

* Research fellow at the Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic

matej.myska@law.muni.cz

The publication of this paper is supported by the Czech Science Foundation – Free Licences Integration Project – registration no. P408/12/2210.

1. INTRODUCTION

Since its introduction by the Directive[1] (further referred as "DRD") the idea of mandatory blanket retention of traffic and localisation data was subject to significant controversy[2] mainly because of its detrimental impact on privacy and telecommunications secrecy. Very simply put these data show who has communicated with whom, from where and for how long. The supporters of data retention – especially the law enforcement agencies (further referred as "LEA") – perceive it as an invaluable tool for combating and investigating of criminal acts.[3] The critiques – recruiting mainly from the human rights watchdog NGOs – denounce it as an invasive, illusory (as regards to proper achievement to the desired aims), illegal, and illegitimate measure.[4] Due to its accession to the European Union in May 2004 this issue had to be dealt with in the Czech Republic. However, the Czech Republic introduced the data retention even before the DRD came into effect. The further development of data retention was a rather rich one and the Czech Republic could be therefore regarded as a perfect role-model country. Similarly as in Germany the relevant implementing provisions had been already declared as unconstitutional by the Czech Constitutional Court (further referred as "CCC") both on the substantive as well as procedural level. Finally the new "revised" legislation regulating data retention has already been introduced.

This paper thus examines all of these aforementioned phases of the data retention implementation in the Czech Republic. However to put the debate in a context, the basic concept and regulation of right to privacy and telecommunication data protection in Czech law are firstly introduced. Part

---

[1] Directive 2006/24/EC of the European Parliament and of the Council of 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. OJ L 105, 13.4.2006, p. 54–63.

[2] See e.g.: ARTICLE 29 Data Protection Working Party Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connect ion with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005) 438 final of 21.09.2005). 1868/05/EN. WP 113.

[3] "These data provide valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice. Their use has resulted in convictions for criminal offences which, without data retention, may never have been solved." Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), COM (2011) 225 final (Apr. 18, 2011). P. 31
Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF. [Accessed Jul 23 2013]

[4] Or as the "unprecedented violation of the fundamental rights of 500 million Europeans." European Digital Rights. Shadow evaluation report on the Data Retention Directive (2006/24/EC). p. 2. Available online: http://www.edri.org/files/shadow_drd_report_110417.pdf. [Accessed Jul 23 2013]

two of this paper explores the evolution of the Czech data retention legislation on two levels, namely the obligation of the operators to retain this data (substantial law) and the entitlement of the LEA to request and use this data (procedural law) including the regulation that was in effect before the Directive. Also the two landmark cases of the CCC striking down the data retention as unconstitutional are discussed. Part four gives an overview of the current data retention regime and discusses the possible weak points. The paper concludes with general thoughts on the state of the data retention in Czech Republic in the European context. It is therefore not the aim of this paper to discuss the DRD in general, its legislative history, related controversies and proportionality itself, as this has been done excellently elsewhere (e.g. Breyer 2005; Bignami 2008; Feiler 2010). Also, the technical details of the data retention are reduced to the needed minimum.[5]

2. THE RIGHT TO PRIVACY AND TRAFFIC AND LOCATION DATA PROTECTION IN CZECH LAW

To understand the following discussion a basics sketch of the interests (rights and freedoms) which could be potentially infringed by the retention of the traffic and location data in Czech law is needed. According to the Art. 1 para. 1 of the Constitution the Czech Republic[6] is a "democratic state governed by the rule of law, founded on respect for the rights and freedoms of man and of citizens." As the Czech Republic is a party to the European Convention on Human Rights the relevant national provisions dealing with the fundamental rights and freedoms to privacy are grounded in its all-encompassing Art. 8. However, the creators of the Czech Charter of Fundamental Rights and Freedoms[7] (further referred as "CFRF") took a more differentiated approach. The respective rights are therefore guaranteed in sev-

[5] For an introductory overview see e.g.: STAMPFEL, Gerald, GANSTERER, Wilfried, ILGER; Michael. Data Retention - The EU Directive 2006/24/EC from a Technological Perspective. Wien : Medien und Recht, 2008. 160 s. ISBN 978-3-900741-53-2. For an excellent in-depth overview see: FISCHER, Johan Conrad. Communications Network Traffic Data Technical and Legal Aspects. ISBN 978-90-386-2339-9.

[6] Constitution of the Czech Republic, No. 1/1993 Coll. (Ústavní zákon č. 1/1993 Sb., Ústava České republiky). Updated English translation available online: http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/prilohy/Ustava_English_version.pdf [Accessed Jul 23 2013].

[7] Resolution of the Presidium of the Czech National Council 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 Coll. (Usnesení č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky). Updated English translation available online: http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/prilohy/Listina_English_version.pdf [Accessed Jul 23 2013].

eral articles of the CFRF. A general safeguard of inviolability of the person and of her privacy is enshrined in the Art. 7 of the CFRF. The Art. 10 para. 1 CFRF specifically provides for protection from any unauthorized intrusion into private and family life. The right to informational self-determination (as coined in the famous "Volkszählung" decision of the German Constitutional Court in 1983[8]) is derived from the Art. 10 para. 2 CFRF that ensures that everyone has "right to be protected from the unauthorized gathering, public revelation, or other misuse of her personal data."

The last particular right to be taken into account within the data retention debate is the right to secrecy of telecommunications which is protected pursuant to the Art. 13. of the CFRF. According to the case law of the CCC the metadata related to the mediated (i.e. indirect) communication shall be regarded as an integral part of such communication and shall be protected as the content.[9] Thus the Art. 13 of the CFRF constitutes the basis for protection of secrecy of dialled numbers and other related data such as date and time of the call, its duration, in case of mobile phone calls also indication of base stations handling the calls. As regards to the operators the general obligation to retain secrecy of the communication is stipulated in the Sec. 89 of the Act No. 127/2005 Coll. (zákon č. 127/2005 Sb., o elektronických komunikacích), further referred as "ECA".

In general the right to privacy is one the most important ones and "enjoys specific respect and protection" as observed by the CCC[10] as it is a necessary prerequisite to a complete and free development of the human personality and society in a liberal state. Lastly, the privacy protection (including personal data protection) cannot be deemed as a rigid concept that is set in stone. Quite to the contrary, the CCC applies the doctrine of evolutive interpretation (as does the European Court of Human Rights)[11] and perceives the right to privacy as an evolving concept. Thus the adequate legal safeguards and protection of privacy should develop alongside the potentially infringing procedures and technologies. The next part should demonstrate that it was not the case as regards to the protection of traffic and location data in the Czech Republic.

---

[8] German Federal Constitutional Court decision of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83.

[9] CCC decision of 22 January 2001, II. ÚS 502/2000.

[10] CCC decision of 2 November 2009, II. ÚS 2048/09.

[11] Decision of the European Court of Human Rights of 25 April 1978 Tyrer v. The United Kingdom, application No. 5856/72, § 31: „The Court must also recall that the Convention is a living instrument […] which must be interpreted in the light of present-day conditions."

3. PAST: THE WAY TO UNCONSTITUTIONALITY

The evolution of the Czech data retention regulation is discussed on the two aforementioned levels. Thus the development of obligation to retain data by the operators is addressed. Next, the corresponding procedural authorisation of the LEA to request and use this data is explained.

3.1. THE OBLIGATION TO RETAIN DATA

The first systematic attempt[12] to use traffic data in the criminal proceedings could be traced back to the Telecommunications Act No. 151/2000 Coll. In its Sec. 86 this law obliged the operators to "inform the authorities entitled pursuant specific law, on facts that are subject to telecommunications secrecy or subject to protection of personal data and traffic data especially any communication of any user at least the past two months."

These data encompassed called and calling number, used service, date, time, duration and location of the communication connection. This exemption to the standard data protection and privacy rules (i.e. non-collection) was introduced on the basis of the exception in the Art. 14 of the Directive 97/66/EC.[13] Interestingly, the reimbursement for such provision of data from the operators was not addressed at all and therefore they had to bear all the related costs.

The "full-scale" data retention regime was introduced by the new ECA. This act became effective law on 1 May 2005 which is almost five months before the Commission even introduced the proposal on the Directive. The Czech legislator namely took advance of the "security exception" in the Art. 15 of the Directive 2002/58/EC.[14] Pursuant to this article Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and Article 8 para. 1, 2, 3 and 4, when such restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications

[12] The previous Telecommunications Act No. 110/1964 Coll. (Zákon č. 110/1964 Sb., o telekomunikacích) contained only obligations related to content wire-tapping.

[13] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. OJ L 24, 30. 1. 1998, p. 1–8.

[14] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31. 7. 2002, p. 37–47.

system, as referred to in Article 13 para. 1 of Directive 95/46/EC. The Sec. 97 para. 3 and 4 ECA contained quite a vague formulation that was in substantive parts linking to the implementing special regulation.[15] This was adopted also in 2005 as the Decree No. 485/2005 Coll., on the extent of traffic and location data, period of time for which such data are retained and manner in which they are submitted to bodies authorised to use the data that laid out the technical details. As will be elaborated further in the part 3.3 the whole data retention regulation could be characterized as very unclear and loose. One prime example was the scope of bodies authorised to request the data. The ECA itself contained a link to the implementing regulation. This however only simple stated in its Section two that the operators must provide the traffic and location data defined by this Decree to the body authorised to request such data, i.e. a rather circular and not precise empowerment. Therefore the authorised bodies had to be derived from provisions in other Acts.[16]

After adoption of the Directive in March 2006 the ECA was amended by the Act No. 247/2008 negligibly,[17] however as regards 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

[15] Full text of the respective provision as translated in the official English version of the annulling CCC Decision:

"Section 97

(3) A legal entities or natural person providing public communications network or providing publicly accessible services of electronic communications is obliged to retain traffic and location data generated or processed within the provision of public telecommunications networks and provision of publicly available services of electronic communications […]. Legal entities and natural persons providing public communications networks or providing publicly available services of electronic communications are obliged to retain traffic and location data regarding unsuccessful call attempts solely under the circumstances when such data is generated and processed and simultaneously retained or recorded. Legal entities and natural persons retaining traffic and location data pursuant the first and the second sentences are obliged to immediately upon request provide such data to the bodies authorised to request such data as set forth by special regulations. Simultaneously such a person is obliged to ensure that the content of the messages and communications is not retained with the data described pursuant to the first and the second sentence. The period for which the data are retained must not be shorter than 6 months and longer than 12 months. Upon expiration of the above period the person retaining the data pursuant to the first and the second sentences is obliged to destroy the data should they have not been provided to the bodies authorised to request such data pursuant to special regulation or unless set forth otherwise by this Act. (Section 90).

(4) The extent of traffic and location data retained pursuant to para. 3, the period for which the data are retained pursuant to paragraph 3 and the form and manner in which they are to be submitted to the bodies authorised to use such data upon request pursuant to special regulation is to be set forth by a statutory instrument".

[16] See the part 3.2 for the list of competent bodies.

[17] The main change was the general obligation to erase the retained data, as well as to ensure its security and quality. Other changes included the administrative duty to report the statistics about usage of the retained data.

SIM cards relations and type of encryption of the communication had to be retained.[18] Quite paradoxically the Czech Republic made use of the exemption stipulated in Art. 15 of the Directive in order to apply de facto a more stringent regime than envisioned by the Directive. Reimbursements of costs incurred by operators in ensuring functionality of the data regime were addressed in Decree No. 486/2005 Sb. Both the costs of acquisition of the needed equipment (CAPEX) as well as the costs related to individual inquiries (OPEX) were covered by the state. By introducing this regime the risk of constitutional challenge from the operators on the grounds of infringement of the right to protection of property was basically eliminated.

3.2. THE EMPOWERMENT TO REQUEST DATA

The development of the retention regulations was not correspondingly followed by the adequate construction of rules how to obtain the retained data. During the effectiveness of the Act Telecommunications Act No. 151/2000 Coll. the Code of Criminal Procedure further referred as „CCP"[19] lacked any specific provisions as regards to the procedural part of handing over to the respective LEA. Thus no specific safeguards or procedures as in the case of "content" wire-tapping were applied – the retained data were simply "requested" from the operators by the Police from the operators. The unconstitutionality of such procedure was declared in the already mentioned decision CCC decision of 22 January 2001, II. ÚS 502/2000. In this particular case the CCC ruled that the metadata about communication generally enjoy the same protection as the content itself. Therefore the LEA should proceed adequately as in the case of the content wire-tapping and all the safeguards for the wiretapped subject should also apply. Specifically, the data request should be limited only for specific crimes, approved by the judge, for limited time, only when this mean brings otherwise unobtainable results (i.e. it is subsidiary and proportionate). The subject should be informed subsequently about wiretapping and able to contest this procedural step. As reaction to this Decision the CCP was amended and new Sec. 88a was added to the legislative text. Again, the formulation was very problem-

[18] A little detail that went unnoticed in both proceedings before the CCC is, that the Decree 485/2005 Coll. stipulated, that also the target fully qualified domain name should be retained. This basically means that also the visited website should be stored which contravenes directly to the Art. 5(2) Directive as content of the communication must not be retained.

[19] Code of Criminal Procedure No. 141/1961 Coll. (Zákon č. 141/1961 Sb., trestní řád), further referred as 'CCP'.

atic and in fact did not consider the aforementioned decisions of the CCC at all. Namely, the retained data could be used and requested for the purpose of "discovering the facts important for the criminal proceedings". The request had to be written, substantiated and authorized by the judge. No other safeguards e.g. the ex post information of the subject were foreseen. Again, despite the adoption of the Directive this provision remained unchanged up until its derogation in 2012. However the Police investigating a crime in the criminal proceedings were not the only "authorised bodies" envisioned in the respective sections of the ECA. Outside the criminal proceedings, the Police could request the retained data pursuant to the Sec. 66/3, 68 and 71 of the Police Act.[20] These sections provide for the authorisation of the Police to request the data in the cases of manhunt/person search and for the performance of the tasks of the special anti-terrorist unit of the Police. The access of Intelligence Services (both civil and military counterintelligence) was disputed as the relevant provisions[21] stipulated only the empowerment to request info about the telecommunication traffic i.e. only the on-going, real time actual connection. Thus the operators were reluctant to hand over the data.[22] Czech speciality [23]was also the access to the retained data by the Czech National Bank pursuant to the Sec. 8/1/d of the Capital Market Area Supervision Act.[24]

3.3. THE CONSTITUTIONAL CHALLENGE AND THE DECISIONS OF THE CZECH CONSTITUTIONAL COURT

Being characterized as totalitarian and non-democratic (Herczeg 2010, p. 30) the national Directive implementation was subject to harsh and constant critique especially from the human rights watchdog NGO Iuridicum Remedi-

[20] Act No. 273/2008 Sb., on the Police of the Czech Republic (Zákon č. 273/2008 Sb., o Policii České republiky).

[21] Act No. 154/1994 Sb., on the Security Information Service (Zákon č. 154/1994 Sb., o Bezpečnostní informační službě) and Act No. 289/2005 Sb., on the Military Intelligence (Zákon č. 289/2005 Sb., o vojenském zpravodajství)

[22] This question was addressed directly in the 'data retention reloaded' as discussed infra in part 4.

[23] The Directive evaluation report does not indicate that other comparable body has access to the retained data, apart from the Hungarian Office for Taxes and Customs. Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), COM (2011) 225 final (Apr. 18, 2011). P. 11.

[24] Act No 15/1998 Coll., on Supervision in the Capital Market Area and on the Amendment of other Act (Zákon č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů) that implements the Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) OJ L 96, 12.4.2003, p. 16–25. However the national Act fails to implement also the paragraph 3 of the Article 12 of this Directive that states that professional secrecy must be preserved.

um.[25] Due to the lack of procedural legitimation and the lack of actual breach of the right to privacy this NGO was not able to file a petition to the CCC. However, the representatives of this NGO managed to convince a group of 51 MPs and Senators[26] to submit a petition to the CCC requesting the abstract review of constitutionality and annulment of the Sec. 97 Art. 3 and 4 of the ECA and the Decree No. 485/2005 Sb. The CCC accepted the formally flawless petition[27] and ruled on it in the decision of 22 March 2011 Pl. ÚS 24/10 (further referred as "Decision I").[28] Firstly, the CCC refused to submit a reference for a preliminary ruling to the Court of Justice of the European Union as the Directive left the Czech legislator enough leeway and could had been implemented in accordance with the Czech constitutional order.[29]

The main declared reason for the complaint was unconstitutionality of these provisions, as they allegedly disproportionately interfered with a constitutionally protected right to privacy in the sense of informational self-determination. Firstly the CCC reminded that the Czech Republic is a democratic rule of law state. Thus the authorities should not intervene with the private sphere of the individual, with the exception of cases "reasoned by a collision with other fundamental rights or public interest, approved in a constitutionally prescribed manner and unambiguously defined by law, and on condition that the intervention anticipated by law is proportional both with respect to the objectives to be attained and the extent of the restriction of the fundamental right or freedom."[30]

Further the CCC defined the right to informational self-determination (informationelle Selbstbestimmung) as "a necessary condition not only for free development and self-realisation of an individual, but also for establishing free and democratic communication rules". The omnipresence of a Big Brother state renders this right as well as the freedom of expression, the right of privacy and the right of the free choice of behaviour virtually non-existent and illusionary.[31] Therefore the restrictions of these rights should be

[25] Home page available: http://www.iure.org/EN [Accessed Jul 23 2013].

[26] Pursuant to the Sec. 64/1/b of the Constitutional Court Act No. 182/1993 Coll. (Zákon č. 182/1993 Sb., o Ústavním soudu).

[27] However did not omit to mention the simple fact that most of the MPs and Senators directly approved the allegedly unconstitutional legislation. § 2 of the Decision I.

[28] For an in-depth analysis of the Decision I see Molek (2012).

[29] Decision I, § 25.

[30] Decision I, § 26.

[31] Decision I, § 30.

applied, due to their importance, "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."[32] To respect the due process principle the individual must be also provided with sufficient guarantees and safeguards against the arbitrary abuse of the state power.

Next the CCC had to assess whether the retention of traffic and location data constitutes an interference with the right to private life and whether the legal regulation of such encroachment is constitutionally conform and respects the aforementioned conditions. In his argumentation the CCC relied heavily on perhaps the most important national decisions regarding the constitutionality of the transposing laws that is the Ruling of the German Federal Constitutional Court of 2 March 2010.[33] The data retention was therefore assessed as a significant interference with right to privacy. Even though the content[34] of the messages is not retained, "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."[35]

Such infringement and limitation of the fundamental rights must therefore strictly respect the constitutional standards. However these are not met by the Sec. 97 para. 3 and 4 ECA and Decree No. 485/2005 Coll., for several reasons. The determination of duties laid upon the operators were evalu-

---

[32] Decision I, § 31.

[33] German Federal Constitutional Court decision of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

[34] The representatives of the Senate did in not even consider such relevance and informational value of the retained data at all. In the preliminary phase of the proceeding in this case their opinion to the issues raised was very straightforward and rudimental:

"The present case did not under any circumstances represent an instance comparable to surveillance and monitoring since the content of the individual phone calls or email messages are not retained and since the internet services are also concerned (...) and solely location and traffic data, in other words technical data are retained."(Decision I, § 14).

This however contravenes directly the opinion expressed by the LEA, e.g. the spokesman of the Czech Security Information Service (Czech Counterintelligence Service) Mr. Jan Šubert who publicly proclaimed:

"In certain cases location data are more worthy than the content of the call itself."

See: ADAMIČKOVÁ & KÖNIGOVÁ, 2011.

[35] Decision I, § 44.

ated as vague and non-specific and thus lacking certainty and clarity.[36] Furthermore the purpose specification under which the data are handed over to the competent bodies is not defined clearly and precisely.[37] Next the missing safeguards against the misuse of the retained data as well as no sanctions to the operators failing to ensure the confidentiality of such data did not respect the rule of law principle. The simple overseeing duty of the Office for Personal Data Protection over the processing of personal data by the operators was found by the CCC to be absolutely insufficient as it is no direct and effective mean of fundamental rights protection.[38] Also the lacking clear rules on security, protection of integrity and confidentiality of the data as well as an explicit duty to discard the data were found to be unconstitutional. As noted by Molek (2012, p. 348) both the answers to the "how" and "why" the data should be provided were not concrete enough for the CCC. For these reasons the contested provision were found ambiguous, not precise and not providing the individual with enough info on the possibility of the state to interfere with its vested fundamental rights and freedoms, .i.e. failing the proportionality step and annulled them. As to the already on-going criminal proceedings the CCC stated that the general courts now shall consider the individual cases one by one from the perspective of the proportionality of the right to privacy infringement. Merely in the form of obiter dictum the CCC questioned the efficacy of the data retention – the main reason being the existence of anonymous SIM cards that are beyond the reach of this tool, but used mainly for committing crimes.[39]

Even though the Decision I dealt also with the Sec. 88a CCP[40] the provision itself had not been contested and therefore could not be also repealed

[36] Decision I, § 46.

[37] […]"to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime"[…]. Decision I, § 47.

[38] Decision I, § 51.

[39] Decision I, § 56.

[40] See Decision I, § 54:

"Beyond the scope of the above, the Constitutional Court needs to emphasise that the deficiencies, as described above and leading to a repeal of the contested provisions, have not been observed in the special legal provisions indirectly referred to in the challenged provisions of Section 97, para. 3 of the Electronic Communications Act. According to the Constitutional Court, it is mainly the afore-mentioned provisions of Section 88a of the Criminal Procedure Code regarding the conditions of using retained data on telecommunications for the purposes of criminal proceedings that fails, by far, to comply with the limits and requirements described above, and therefore it also seems unconstitutional from the Constitutional Court's perspective. Nevertheless, due to the fact that it was not contested by the applicant in the petition, the Constitutional Court deems necessary to invite the legislature to consider amending, as a consequence of repealing the challenged provisions, Section 88a of the Criminal Procedure Code so that it complies with the constitutional order."

as the CCC does not rule ultra petitutm (Molek 2012, p. 350). This was however done in the proceedings concerning the handing over of traffic and location data to the Military Police before the District Court in Prague 6. This court that had to authorized a data request order found out that it could not authorize such request as it would had been inconsistent with the constitutional order of the Czech Republic.[41] The proceeding was therefore stayed and a petition was filed with the CCC. In its assessment in Decision of 22 December 2011, Pl. ÚS 24/11 (further referred as "Decision II") CCC relied logically mainly on the reasoning presented in Decision I, as discussed above. The purpose limitation of data retention, i.e. its intended usage for "discovering the facts important for the criminal proceedings" proved to be the crucial breaking point. Such blurry delimitation of the encroachment of the fundamental right to privacy and informational self-determination was regarded as completely lacking a reflection of the principle of proportionality. Consequently, the requesting of retained data was used as a common tool for obtaining electronic evidence rather than a subsidiary and exceptional one. Also the missing safeguards and direct remedies for the individuals were missing. Thus the Sec. 88a CCP was also annulled with the effectiveness postponed to 30. 9. 2012. Judge Janů presented in its dissent a unique opinion on the priority of the constitutionally conform interpretation of the contested provision rather than a simple formal derogation. The needed argumentation could be found in the already mentioned CCC decision of 22 January 2001, II. ÚS 502/2000. According to this decision, the retained data should be requested and used under similar circumstances as content wire-tapping.

Immediately after the repeal of the relevant "data retention" provisions a period of uncertainty had arisen. The operators had no obligation to retain the traffic and location data, however the LEA still had the procedural empowerment to ask for them – Decision II annulling the Sec. 88a CCP had postponed effectiveness till 30. 9. 2012. The operators thus started to be very reluctant to hand out data referring to the Decisions I and II. Consequently the LEA representative stated that they have practically had "gone blind" and without means to investigate and prosecute crimes effectively.[42] In reality they tried to at least to get access to "billing data" as provided in the Sec. 90 ECA or tried the way of general obligation to cooperate with Police as

[41] Due to the reason explained in Decision I.

[42] See Chaloupská & Berná, 2011.

stipulated in Sec. 8/1 CCP. The general discontent with the rather chaotic delimitation of the obligations and duties related to data retention, the potential Art. 258 TFEU infringement procedure, as well as the clearly set timeframe to re-implement the DRD led the Czech government to opt for a new legislation amending the ECA, CCP and other related acts.

4. PRESENT: DATA RETENTION RELOADED

The work on the amendment began shortly after the Decision II of the CCC. On 27 February 2012 the Czech government presented the new data retention legislation as the Print of the Chamber of Deputies No. 615/0. Without any procedural delays the proposal was passed and made its way to the Senate. This legislative body also gave the proposal a go on 18 July 2012 and finally the President signed the bill on the 1 August 2012. The bill was published in the Collection of Laws as the Act No. 273/2012 Sb. amending Act No. 127/2005 Sb., On electronic communications and on amendment to some related laws (Electronic Communications Act), as amended, and certain other laws (further referred as the "AA")[43] and became effective law on 1 October 2012. The technical details were prescribed by the implementing Decree No. 357/2012 on storing, handing over and liquidation of traffic and location data[44] and was published and became effective on 1 November 2012.

As the data retention was struck down on the two above mentioned levels (retaining and requesting of the data) the AA had to relevantly address both of the issues and respect the boundaries set forth by the CCC at the same time. As the CCC in its decision laid out quite clearly what the contested legislation was missing the needed work was very simplified. The comments of the CCC had to be simply put into a legislative text. Thus the AA is divided into five substantial parts. The first part deals with the reformulating of the Sec. 97 ECA. As regards to the obligation of the operators to retain the data the new wording now entails a taxative enumeration of the subjects empowered to request the data. These include the Police bodies, Security Information Service; Military Intelligence and Czech National Bank. Next in order to fulfil other requirements of the CCC the clear obligation to

[43] Zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony

[44] Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

ensure the security and confidentiality of the retained data, as well as to destroy them in an irreversible manner was set out in the Sec. 88a ECA. Non-compliance with these provision is regarded as an administrative offence and punishable by fine up to CZK 10.000.000,- (approximately EUR 400.000). The second part of the novelisation focused on the procedural part of data retention and reshapes the Sec. 88a CCP to respect the principle of proportionality and subsidiarity. Data retention (as a mean of criminal investigation) should be used "only if the objective pursued cannot be achieved by other less invasive means".

Also the types of crime for which the retained data could be requested were refined. General requirement is that the prosecuted crime should be an intentional one for which the law provides for imprisonment with an upper limit of the penalty of at least three years. This however does not apply on the exhaustive list of the crimes, which cannot be practically prosecuted without the traffic and location data, i.e. crimes committed by means of electronic communication.[45] As the Explanatory Memorandum[46] to the Amendment explains "should the police during investigation of these crimes had no chance to get traffic and location data, one could consider the decriminalization of such conduct, as these crime would be virtually inexplicable".[47]

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. The concerned individual should have, according to the new legislation, the same means of protection as in the case of content wire-tapping. This means a subsequent information about the fact that the data retention has been employed and the possibility of complaint against such procedure to the Supreme Court of the Czech Republic. The third and fifth part of the novelisation entail and introduce the specific empowerment of the Intelli-

[45] The full list with relevant section of the Penal Code No. 40/2009 Coll. (Zákon č. 40/2009 Sb., trestní zákoník) include 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).

[46] 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: http://www.psp.cz/sqw/text/orig2.sqw?idd=84557 [Accessed Jul 23 2013].

[47] Ibid, p. 22.

gence Services to request the traffic and location data from the operators in the form and way specified by the Decree upon approval from the Higher Court in Prague. The fourth part regulates again the Czech speciality that is ability to request data by the Czech National Bank.

As was noted above, the AA was modelled closely after the Decision I and II and thus should reflect fully the proportionality principle. However in its critical remarks to the AA the NGO IuRe (Vobořil, 2012) responsible for overthrowing the original data retention pointed out that the institute per se is not effective. Moreover the other methods how to obtain the data without approval of the judge remained untouched – that is pursuant to the Sec. 68 and 71 of the PA. It is indeed questionable, why should the Security Information Service, that has to perform basically the same tasks, should need the approval of the judge whereas the anti-terror unit of Police should not. Certain reservations were expressed also against the implementing Decree. Again the devil was in the detail and as regards to the server services not only the source of the communication should have been stored but also the target of the request which would basically mean the storing of the communications.[48] Finally the timing of the Amendment in general seems to be rather problematic. The Directive itself, as will be elaborated in the next part, is now under the scrutiny of the Court of Justice of the European Union and thus the Czech new regulation of data retention may easily end up in discord with the forthcoming decision of the Court.

5. FUTURE: WAITING FOR THE COURT OF JUSTICE OF THE EUROPEAN UNION

The balancing of data retention for security purposes and human rights seems to be an on-going struggle since the introduction of this crime investigation tool. It remains however unclear, whether the new Czech data retention legislation will not be contested before the CCC again. The simple fact that the current regime is closely modelled upon the Decisions I and II does not leave much space for argumentation against the "data retention reloaded" itself as the CCC would practically contradict its opinions on the proportionality of such fundamental rights encroachment. As noted by Molek (2012, p. 352) the CCC, by denying the motion for sending a preliminary reference to the CJEU, also closed the gate for answering the question whether the Directive itself is compatible with the general right to privacy

[48] Inital version of the implementing AA Decree, that was later published as 357/2012 Coll.

and data protection.[49] This was however done by other national courts, namely the Irish High Court (Case C 292/12 Digital Rights Ireland) and Austrian Federal Constitutional Court (Case C-594/12 Seitlinger et al.). In both proceedings the referring courts asked the CJEU basically to consider the proportionality of the Directive as such and its compatibility with the Articles 7, 8 and 11 of the Charter of Fundamental rights of the European Union. As both cases do thematically overlap, the CJEU co-joined the oral hearing on these cases that was held on 9 July 2013. In questions sent out beforehand to the invited parties (including the representatives of the respective states and European Data Protection Supervisor) the CJEU asked core questions dealing with the necessity and proportionality of the Directive. According the first reactions and round-ups the oral hearing[50] it could be stated that the CJEU took a rather sceptic approach and was not fully convinced that the Directive, i.e. the data retention is and effective and necessary tool for crime detection and prosecution. Even though the LEA claim the necessity of such data the current statistics do show the opposite. The survey of Max-Planck Institute (Albrecht et al., 2011, p. 219) shows that there is no direct correlation between the absence data retention and clearance rate of the crimes. Further the most current data from Austria do tell us that in fact the data retention is used rather only for petty crimes.[51] Also the simple statistics comparing the clearance rate of crimes before and after the annulment of data retention regime in the Czech Republic do not show any significant drop after the annulment of the respective provisions.

Year	**2009**	**2010**	**2011**	**2012**
Number of crimes	332839	313387	317177	304528

[49] Molek (2012, p. 351) even labelled the CCC as hypocritical for striking down the implementation without contesting the Directive itself.

[50] LOHNINGER, Thomas. Live-Ticker: Anhörung des Europäischen Gerichtshofs über die Richtlinie zur Vorratsdatenspeicherung [online]. Netzpolitik.org. Issued 9. 7. 2013. Available in German: https://netzpolitik.org/2013/live-ticker-vom-eugh-verfahren-gegen-die-vorratsdatenspeicherung/.

[51] These statistics were presented during the oral hearing before the CJEU. As noted by EDRi: "Between 1 April 2012 and 31 March 2013 retained data has been accessed by Austrian prosecutors in 326 cases. Out of these 326 cases, 139 are already closed. In 56 of these 139 cases, the data retained contributed to solving the case. The offences of these cases were: theft (16), drug offences (12), stalking (12), fraud (7) and others" KIRSCH, Andreas. EDRi-gram newsletter - Number 11.14, 17 July 2013. Data retention: "We ask the Court to rule in favour of Freedom". Available online:The original stats are also available in German: http://www.parlament.gv.at/PAKT/VHG/XXIV/AB/AB_14397/imfname_314525.pdf [Accessed Jul 23 2013].

Year	2009	2010	2011	2012
Cleared crimes	127604	117685	122238	120168
Clearance rate in %	38.34%	37.55%	38.54%	39.46%

Overview of crimes recorded/cleared in Czech Republic in 2009-2012[52]

The "Czech way" of dealing with the DRD implementation may have provided for a valuable lesson for states[53] dealing or about to deal with the constitutionality of its own national data retention legislation. However, the Czech legislator should have waited for the results of the proceedings before the CJEU. Being one step ahead before the EU, as it seems to be the Czech tradition in the case of data retention, will bring only disharmonised results and further expenses. As the heading of this part implicates the final decision as regards to further fate of the data retention in Czech Republic (and also in Europe) is now in the hands of the CJEU and could be only awaited eagerly. For the time being the next most important milestone will be the opinion of the Advocate General that should be filed on 7 November 2013. If the General Advocates takes into consideration the current statistics as well as the legal doctrine (Breyer, 2005; Feiler, 2010; Otto & Seitlinger, 2006; Derksen, 2011) the overall gist of the answers to the questions referred should be quite simple – the Directive is not compatible with the Art. 7 and 8 of the Charter of the Fundamental Rights of the European Union. Consequently the Czech implementation should be also deemed unconstitutional.

REFERENCES

ADAMIČKOVÁ, Naďa; KÖNIGOVÁ, Marie. Tajné služby pošilhávají po výpisech z mobilů, a to až půl roku zpět. Novinky.cz. 23 August 2011. Available online in Czech: <http://www.novinky.cz/domaci/242519-tajne-sluzby-posilhavaji-po-vypisech-z-mobilu-a-to-az-pul-roku-zpet.html> [Accessed Jul 23 2013].

[52] Statistics are published annually online at: http://www.policie.cz/statistiky-kriminalita.aspx [Accessed Jul 23 2013].

[53] For example Slovakia where the NGO European Information Society Institute (www.eisionline.org) choose a similar way as the Czech NGO IuRe. See: Data Retention before the Slovak Constitutional Court. http://www.eisionline.org/index.php/projekty-m/data-retention-m/49-slovak-case-on-data-retention [Accessed Jul 23 2013].

ALBRECHT, Hans Jörg et al. Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenab- wehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikations-verkehrsdaten. Gutachten der kriminologischen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht im Auftrag des Bundesamtes für Justiz zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung [online]. Freiburg i.Br., Juli. 2011. 2., erweiterte Fassung, 271 p. Available online: <http://www.mpg.de/5000721/vorrats-datenspeicherung.pdf>. [Accessed Jul 23 2013].

BIGNAMI, Francesca. Privacy and Law Enforcement in the European Union: The Data Retention Directive. Chicago Journal of International Law 2011, Vol. 8, No. 1. p. 233-255.

BREYER, Patrick. Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. European Law Journal. May 2005, Vol. 11, pp. 365-375.

CHALOUPSKÁ, Markéta; BERNÁ, Veronika. Policie: Oslepli jsme, nesmíme lidi sledovat přes mobil. Lidovky.cz. 29 May 2011. Available online: http://www.lidovky.cz/policie-oslepli-jsme-nesmime-lidi-sledovat-pres-mobil-pfi-/zpravy-domov.aspx?c=A110529_134727_ln_domov_mev [Accessed Jul 23 2013].

DERKSEN, Roland. Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta. WD 11 – 3000 – 18/11, 25. 2. 2011 [cit. 2012-06-30]. Available online in German: http://www.vorratsdatenspeicherung.de/images/rechtsgutachten_grundrechtecharta.pdf [Accessed Jul 23 2013].

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: http://www.psp.cz/sqw/text/orig2.sqw?idd=84557 [Accessed Jul 23 2013].

FEILER, Lukas. The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. European Journal of Law and Technology, Vol. 1, Issue 3, 2010.

FISCHER, Johan Conrad. Communications Network Traffic Data Technical and Legal Aspects. ISBN 978-90-386-2339-9.

HERZCEG. Jiří. Ústavněprávní limity monitoringu telekomunikačního provozu. Bulletin advokacie. 2010, č. 5, s. 22-31. ISSN 1210-6348.

KIRSCH, Andreas. EDRi-gram newsletter - Number 11.14, 17 July 2013. Data retention: "We ask the Court to rule in favour of Freedom". Available online: The original stats are also available in German: http://www.parlament.gv.at/PAKT/VHG/XXIV/AB/AB_14397/imfname_314525.pdf [Accessed Jul 23 2013].

MOLEK, Pavel. Czech Constitutional Court: Unconstitutionality of the Czech Implementation of the Data Retention Directive, Decision of 22 March 2011, Pl. ÚS 24/10. European Constitutional law Review, Cambridge: Cambridge University Press, 2012, Vol. 8, Issue. 2, p. 338-353. ISSN 1574-0196.

OTTO, Gerald; SEITLINGER, Michael. Die „Spitzelrichtlinie“. Medien und Recht. 2006, č. 4. S. 227-234. ISSN 0257-3822.

STAMPFEL, Gerald, GANSTERER, Wilfried, ILGER; Michael. Data Retention - The EU Directive 2006/24/EC from a Technological Perspective. Wien : Medien und Recht, 2008.

VOBOŘIL, Jan. Výhrady iure k novele zákona o naší komunikaci. 27. 3. 2012. Available online in Czech: <http://slidilove.cz/sites/default/files/vyhrady_iure_-_provozni_a_lokalizacni_udaje_-_snemovni_tisk_c._615.pdf>. [Accessed Jul 23 2013].