2011/03/22
Pl. ÚS 24/10
94/2011 Coll.

The Czech Republic
Constitutional Court
Judgment
In the Name of the Republic

The plenary session of the Constitutional Court attended by Stanislav Balík, František Duchoň, Vlasta Formánková, Vojen Güttler, Pavel Holländer, Vladimír Kůrka, Dagmar Lastovecká, Jan Musil, Jiří Nykodým, Pavel Rychetský, Miloslav Výborný a Eliška Wagnerová (judge – rapporteur) decided on March 22, 2011 on a proposal filed by a group of Members of Parliament of the Czech Republic represented by Marek Benda, registered office Prague 1, Sněmovní 4, to repeal Section 97, subsections 3 and 4 of the Act on Electronic Communications and on Amendment to Certain Related Acts (Electronic Communications Act) No. 127/2005 Coll., as amended, and to repeal Decree No. 485/2005 Coll. on the Extend of Traffic and Location Data, the Time of Retention Thereof and the Form and Method of the Transmission Thereof to Bodies Authorised to Use such Data, in the presence of Chamber of Deputies and Senate of the Parliament of the Czech Republic as parties involved, as follows:

Provisions of the Act on Electronic Communications and on Amendment to Certain Related Acts (Electronic Communications Act) No. 127/2005 Coll., as amended, Section 97, Subsections 3 and 4 of, and Decree No. 485/2005 Coll. on the Extend of Traffic and Location Data, the Time of Retention Thereof and the Form and Method of the Transmission Thereof to Bodies Authorised to Use such Data, shall be repealed as of the day of promulgation of this judgment in the Collection of Laws.

Grounds of the Decision:
I. Proposal Recapitulation
...

II. Recapitulation of the Briefs from the Parties

...

III. Waiving Oral Proceedings

...

IV. Constitutional Conformity of the Procedure of Passing Contested Provisions and Legal Conditions for Passing the Contested Decree

...

V. Wording of contested Provisions of the Act and Contested Decree

...

VI. Preliminary Question

25. Primarily, the Constitutional Court had to consider the proposal filed by petitioners to submit the European Court of Justice preliminary question pursuant to Article 234 of the Treaty Establishing the European Community questioning the validity of Data Retention Directive, since there is a significant risk that the Data Retention Directive transposed into Czech law by contested provisions and contested Decree contradicts the law of the European Community. In this respect, the Constitutional Court emphasizes that even after the accession of the Czech Republic to the EU (since 1. May, 2004), the norms of the constitutional order of the Czech Republic still represent the reference framework for Constitutional Court´s reviews, since the Constitutional Court´s task is to protect constitutionality (Article 83 of the Constitution of the Czech Republic) in both aspects of it, i.e. protection of objective constitutional law as well as subjective rights, i.e. fundamental rights. *Acquis communautaire* does not form a part of the constitutional order and therefore, the Constitutional Court is not competent to interpret it. However, the Constitutional Court cannot fully ignore the effect *acquis communautaire* has on making, implementing and interpreting national law, namely regarding legal regulations which are directly linked to *acquis communautaire* with respect to origin, effect and purpose [cf. Constitutional Court judgments File No. Pl. ÚS 50/04 of 8 March, 2006 (N 50/40 SbNU 443; 154/2006 Coll.), File No. Pl. ÚS 36/05 of 16 January, 2007 (N 8/44 SbNU 83; 57/2007 Coll.) or File No. II. ÚS 1009/08 of 8 January, 2009 (N 6/52 SbNU 57)]. 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,

since particular provisions only define the obligation to retain such data. As far as transposition is concerned, the purpose of the Directive has to be attained; yet particular provisions of the act and subordinate legislation related to retaining and handling data including measures preventing misuse of such data, a certain constitutional standard has to be met arising from the Czech constitutional order as interpreted by the Czech Constitutional Court. The reason for this is the fact that this particular form of transposition – i.e. contested provisions of the act and subordinate legislation – represent declaration of the will of the Czech legislator and could have varied while still meeting the purpose of the Directive in terms of selected instruments; at the same time, the legislator was bound to respect the constitutional order when making such selection.

VII. Points of Reference for Considering the Proposal

VII. A) Right to Respect for Private Life and Informational Self-Determination

26. Article 1, paragraph 1 of the Constitution of the Czech Republic incorporates the normative principle of democratic law-abiding state. The fundamental attribute of the constitutional concept of a law-abiding state and prerequisite of its functioning is respect towards fundamental rights and freedoms of an individual which is explicitly specified as an attribute of the chosen constitutional concept of law-abiding state in the above mentioned constitutional provision. This constitutional provision forms the basis for the material concept of legal statehood which is characterised by public authority respecting free (autonomous) sphere of the individual defined by fundamental rights and freedoms; as a matter of principle, public authority does not intervene in this sphere, or more precisely only in cases where such intervention is justified by conflict with other fundamental rights, that is in public interest which is in conformity with the constitution and which is unambiguously defined by law providing that the intervention anticipated by law respects the proportionality principle with respect to aims that are to be attained as well as the extent of reduction of fundamental right or freedom.

27. The concept of privacy is mostly being brought into connection with Western culture, more accurately with Anglo-American cultural concept in the context of liberal political philosophy. This concept is apparently not commonly shared in terms of emphasis placed on the importance of privacy as well as the question to what extend should privacy be protected.

There are different concepts in different cultures concerning the issue of level of privacy individual persons have the right to in various contexts. However as soon as 1928, Judge Brandeis declares the following opinion on privacy in the frequently quoted dissent (Olmstead v. U. S., 438, 478, 1928): "The makers of our Constitution understood the need to secure conditions favourable to the pursuit of happiness (…) and include the right (…) to be left alone – the most comprehensive of rights and the right most valued by civilized men." And thus a right to privacy not explicitly mentioned by the constitution has gradually become fundamental structural element of the constitution of the U.S., safeguarding autonomy of the individual, even though its exertion is still subject to disputes within the U.S. Supreme Court.

28. The need for respecting individual ways of living has become, together with the claim to respect one´s life, physical and spiritual integrity, personal freedom and property, one of the central human rights claims for autonomy of individuals which has formative impact on European national (fundamental) human rights catalogues as well as their subsequent regional and universal counterparts. However, not even the original European national catalogues of fundamental rights did explicitly mention the right to privacy or private life as such, as documented by the wording of national constitutions dating back to 1940s and 1950s (e.g. the constitution of the Federal Republic of Germany, not mentioning Austria, constitutions of Denmark, Finland as well as France, Ireland and also Italy and other states). The requirement to respect privacy and privacy protection are closely linked to the development of technical and technological possibilities, which of course increase the level of freedom threatening the potential of the state.

29. As the Constitutional Court stated in judgment File No. II. ÚS 2048/09 of 2 November, 2009 (available in the electronic judgment database http://nalus.usoud.cz): "fundamental right to undisturbed private life of an individual enjoys particular respect and protection in liberal democratic states (Article 10, paragraph 2 of the Charter of Fundamental Rights and Freedoms, No. 2/1993 Coll. (hereinafter the Charter))". The right to respect for private life functions primarily as a guarantee of space for development and self-fulfilment of individual personality. Together with the traditional concept of privacy in terms of special dimension (protection of home in broader sense) and in connection with autonomous existence of development of social relations undisturbed by public authority (within marriage, family, society), the right to private life incorporates also a guarantee of self-determination in terms of crucial decisions being made by the individual. In other words, the right to privacy also

guarantees the right of an individual to decide at one´s own discretion if and to which extend, in what ways and under which circumstances should personal private facts and information be disclosed to other entities. This is an aspect of the right to privacy in form of the right to informational self-determination guaranteed explicitly by Article 10, paragraph 3 of the Charter [cf. Constitutional Court judgment File No. IV. ÚS 23/05 of 17 July, 2007 (N 111/46 SbNU 41) and File No. I. ÚS 705/06 of 1 December, 2008 (N 207/51 SbNU 577) or Federal Constitutional Court of Germany decision of 15 December, 1983 BVerfGE 65, 1 (*Volkszählungsurteil*) or 4 April, 2006 BVerfGE 115, 320 (*Rasterfahndungurteil II*)].

30. When reviewing constitutionality of legal regulation concerning data collection and retention process for the purposes of census (*Volkszählung*), the Federal Constitutional Court of Germany i. a. stated in the decision BVerfGE 65, 1, mentioned above, that in modern society characterised among others by enormous rise in the amount of information and data, individuals have to be protected against unlimited collection, retention, use and disclosing of data concerning one´s person and privacy within the scope of a more general right of an individual to privacy guaranteed by the constitution. Should individuals not be guaranteed the possibility to guard and control the contents as well as scope of personal data and information provided which are to be disclosed, retained or used for other than their original purposes, should they not have the possibility to identify and access reliability of their potential communication partners and adjust their actions accordingly, then this is inevitably a case of infringement or restriction of their rights and freedoms and therefore, one can in such case not speak of free and democratic society. The right to informational self-determination (*informationelle Selbstbestimmung*) thus represents a fundamental prerequisite not only for the free development and fulfilment of an individual within the society but also for the set up of a free and democratic communication system. In simple words, under omniscient and omnipresent state and public authority, the freedom of expression, right to privacy and free choice concerning one´s behaviour and actions become basically non-existent and illusory.

31. The Charter does not guarantee the right to respect for private life under one comprehensive Article (as is the case with Article 8 of the Convention). On the contrary, the protection of private sphere of an individual is divided within the Charter and amended by further aspects of the right to privacy as declared in several passages of the Charter (e.g. Article 7, paragraph 1, Articles 10, 12 and 13 of the Charter). In the same way, the right to informational self-determination as such can be derived from Article 10, paragraph 3 of the

Charter, which guarantees individuals the right to protection from unauthorised collection, disclosure or other misuse of data concerning one´s person, and that together with Article 13 of the Charter, safeguarding privacy of correspondence and conveyed messages, whether kept in private or send by mail, communicated by telephone, telegraph or any other similar devices or ways. However, such "fragmentation" of legal regulation concerning aspects of privacy of an individual cannot be overestimated and the list of issues that "fall" under the right to privacy and private life cannot be regarded as exhaustive or definitive. When interpreting single fundamental rights which reflect the right to privacy in its various dimension as specified in the Charter, it is necessary to respect the aim of the right to privacy in terms of general concept of it and constantly evolving nature as such, i.e. it is necessary to consider the right to private life within the context of the given time period. Thus the right to informational self-determination, guaranteed under Article 10, paragraph 3 and Article 13 of the Charter, has to be interpreted with respect to rights guaranteed under Articles 7, 8, 10 and 12 of the Charter in particular. Given its nature and importance, the right to informational self-determination falls within the scope of fundamental human rights and freedoms, since together with personal freedom, freedom in terms of spatial dimensions (home), freedom of communication and certainly other fundamental rights guaranteed under the constitution, it creates the personal sphere of an individual, whose individual integrity has to be respected and consistently protected as necessary grounds for dignified existence and development of human life as such; therefore, it is certainly justified to guarantee respect and protection of this sphere under constitutional order because – looking at this issue from a slightly different point of view – this represents the manifestation of respect for rights and freedoms of humans and citizens (Article 1 of the Constitution of the Czech Republic.)

32. It is clear, following the consistent judicature of the Constitutional Court especially in relation to the issue of wiretapping, that protection of the right to respect for private life in the form of right to informational self-determination pursuant to Article 10, paragraph 3 and Article 13 of the Charter does not only apply to the contents of messages conveyed via telephone, but to data concerning dialled numbers, dates and times of calls, duration, and in case of mobile phones, data on base stations handling calls [cf. e.g. judgment File No. II. ÚS 502/2000 of 22 January, 2001(N 11/21 SbNU 83): "Everybody´s privacy deserves substantial (constitutional) protection not only in connection with the contents of conveyed messages as such, but also with respect to the above mentioned data. It can therefore be stated that Article 13 of the Charter 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. (...) Such data form an integral part of telephone communication"; or similarly cf. judgement File No. IV ÚS 78/01 of 27 August, 2001 (N 123/23 SbNU 197), File No. I. ÚS 191/05 of 13 September, 2006 (N 161/42 SbNU 327) and File No. II. ÚS 789/06 of 27 September 2007, (N 150/46 SbNU 489)].

33. The above mentioned judgments of the Constitutional Court are i. a. based on the judicature of the European Court of Human Rights [Malone v. UK decision (No. 8691/79 of 2 August, 1984) in particular] which deduces from Article 8 of the Convention, guaranteeing the right to respect for private and family life as well as home and correspondence, also the right to informational self-determination, as the Court repeatedly emphasised that data collection and retention related to private life of an individual fall within the scope of Article 8 of the Convention, since the term "private life" cannot be interpreted restrictively. From this point of view, right to privacy thus incorporates the right to protection from being monitored, watched and followed by public authority as well and that even in public areas or areas open to the public. Moreover, there is no essential reason for which to exclude professional, commercial or social activities from the term private life [cf. Niemietz v. Germany decision (No. 13710/88 of 16 December, 1992]. As declared by the European Court of Human Rights, such extensive interpretation of the term "private life" is in accordance with the Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (elaborated by the Council of Europe as of 28 January, 1981, effective in the Czech Republic since 1 November, 2001, published in the Collection of International Treaties under No. 115/2001 Coll.), the purpose of which is to "secure in the territory of each Party for every individual (…) respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1) while these are defined as „any information relating to an identified or identifiable natural person" (Article 2) [cf. Amman v. Switzerland decision (No. 27798/95) of 16 February, 2000 and jurisdiction quoted there].

34. In its judicature related to the right to respect for private life pursuant to Article 8 of the Convention, the European Court of Human Rights described actions such as data, contents of mail control and wiretapping as infringement of privacy of an individual [cf. Klass and others v. Germany decision (No. 5029/71) of 6 September, 1978, Leander v. Sweden decision (No. 9248/81) of 26 March, 1987, Kruslin v. France (No.11801/85) of 24 April, 1990 or Kopp v.

Switzerland decision (No. 23224/94) of 25 March, 1998], detecting telephone numbers of persons on the telephone [cf. P. G. and J. H. v. UK decision (No. 44787/98) of 25 September, 2001], detecting data concerning telephone connection (cf. the above mentioned Amman v. Switzerland decision) or retaining DNA data in databases of individuals charged with an offence [cf. S. and Marper v. UK decision (No. 30562/04 and 30566/04) of 4 December, 2008]. In the Rotaru v. Rumania decision (No. 28341/95) of 4 May, 2000, the European Court of Human Rights deduced positive obligation of the state to discard data relating to private sphere of an individual, which were collected and processed by the state, from the right to private life manifested through the right to informational self-determination.

35. Similar approach is traceable in the judicature of constitutional courts of other countries as well. For instance the above mentioned Federal Constitutional Court of Germany guarantees – via the right to informational self-determination – protection not only of the contents of information conveyed but also external circumstances under which communication takes place – i.e. place, time, participants, type and way of communication – since such information concerning the circumstances of a given communication can, combined with other data, indicate the communicated contents as such; when inspecting and analyzing this data, it is possible to create individual profiles of participants involved in the communication [cf. decision of 27 July, 2005, BVerfGE 113, 348 (Vorbeugende Telekommunikationsüberwachung) or 27 February, 2008, BVerfGE 120, 274 (Grundrecht auf Computerschutz)].

VII. B) Admissibility of Infringement of the Right to Informational Self-Determination

36. Protection against security threats and the need to secure the availability of such data for purposes of precaution, detection, investigation and prosecution of serious crimes carried out by public authority is usually declared as the primary purpose of legal regulation of universal and preventive collection and retention of traffic and location data on electronic communication. As previously repeatedly emphasised by the Constitutional Court, prosecution of crimes and justified punishment of offenders is a public interest approved by the Constitution, the essence of which being the delegation of the responsibility to hold offenders responsible for substantial fundamental rights and freedoms infringement by natural persons and legal entities to the state. Should the criminal law allow carrying out public interest in prosecution of criminality by means of robust instruments, the use of which results

in serious infringement of personal integrity and fundamental rights and freedoms of an individual, then legal constitutional limit must be respected while such enforcement takes place. Infringement of personal integrity and privacy (i.e. absence of respect for it) can thus occur only extremely exceptionally on the part of public authority, should this be inevitable in a democratic society in case that the purpose of public interest cannot be reached in any other way and should this be acceptable in terms of legal existence and compliance with effective and specific guarantees against arbitrariness. An individual has to have sufficient guarantees and warrantees against possible misuse of power on the part of public authority in order for essential prerequisites of a fair trial to be met. Such necessary guarantees comprise of adequate legal regulation and existence of effective control of compliance with it, this being primarily the inspection of the most significant infringement of fundamental rights and freedoms of individuals by an independent and impartial court, since courts are bound to protect fundamental rights and freedoms of individuals (Article 4 of the Constitution of the Czech Republic) [cf. judgment File No. I. ÚS 631/05 of 7 November, 2006 (N 205/43 SbNU 289) a File No. Pl. ÚS 3/09 of 8 June, 2010 (219/2010 Coll., available in the electronic judgment database http://nalus.usoud.cz)].

37. The Constitutional Court was more specific on compliance with the conditions described above in its judicature when considering the admissibility of infringing privacy of individuals on the part of public authority in form of wiretapping telecommunication [cf. e.g. judgments File No. II. ÚS 502/2000, File No. IV. ÚS 78/01, File No. I. ÚS 191/05 (see above) or judgment File No. I. ÚS 3038/07 of 29 February, 2008 (N 46/48 SbNU 549)]. The right of an individual to privacy in the form of right to informational self-determination pursuant to Article 10, paragraph 3 and Article 13 of the Charter can on the grounds of precaution and protection against criminal activity be infringed only pursuant to imperative legal regulation which must be in compliance with requirements resulting from the principle of law-abiding state fulfilling requirements resulting from the proportionality test; should fundamental rights or freedoms be in conflict with public interest or other fundamental rights and freedoms, the purpose (aim) of such infringement has to be considered with regard to instruments employed, the principle of proportionality (in its broader sense) being the criterion of such considerations. Such legal regulation has to be precisely and clearly formulated as well as predictable to a satisfactory extend in order to provide potentially affected individuals sufficient information about circumstances and conditions under which is the public authority entitled to infringe their privacy, so that they can adequately adjust their behaviour in such a

way as to avoid conflict with the present rule. Similarly, there has to be a strict definition of powers delegated to the authorities in question, ways and rules of exercising it so that individuals are granted protection against arbitrary infringements. Three criteria are involved in reviewing admissibility of particular infringements in terms of the proportionality principle (in broader sense). First of all, the prospects to meet the purpose have to be considered (or suitability); this covers reviewing whether desired purpose – being the protection of other fundamental right or public goods – can ever be attained with such measure. Secondly, the necessity has to be assessed, considering whether the chosen measure is the most moderate one with respect to the fundamental right. And finally, adequacy has to be examined (in the narrow sense), i.e. whether the fundamental right infringement is not inadequate in relation to the desired purpose, meaning that adverse effects resulting from measures infringing fundamental human rights and freedoms cannot, in case that fundamental right or freedom conflicts with public interest, exceed positive effects represented by public interest with respect to these measures [cf. judgment File No. Pl. ÚS 3/02 of 13 August, 2002 (N 105/27 SbNU 177; 405/2002 Coll.)].

38. Essential requirement for juridical protection of fundamental rights, in case of application of criminal law measures infringing fundamental rights and freedoms of individuals, is manifested in particular by issuing judicial warrants and supporting it with sufficient reasoning. This has to be in compliance with legal requirements and constitutional principles on which the legal provision is based in particular, or as the case may be, which in reverse limit its interpretation since applying such principle represents very serious infringement of fundamental rights and freedoms of every individual. "Judicial wiretapping and telecommunication recording warrant can be issued only in properly initiated criminal proceedings for criminal activity qualified under law and must be supported by relevant evidence which indicates justified suspicion that a crime has been committed. The warrant has to be personalised in relation to a specific person that uses the telephone station. And finally, the warrant has to, at least to a certain level, specify which facts relevant for criminal proceeding are to be revealed using such means and the presumptions for thereof" (cf. quote Constitutional Court judgments File No. II. ÚS 789/06 and File No. I. ÚS 3038/07 – for both see above).

39. In its judicature, the European Court of Human Rights advocates a similar approach. European Court of Human Rights, in accordance with Article 8, paragraph 2 of the

Convention, which sets legal constitutional limits for infringement of fundamental rights and freedoms of individuals guaranteed under Article 8, paragraph 1 of the Convention, considers in every individual case primarily whether the alleged infringement or restriction of fundamental rights and freedoms can be covered by Article 8 of the Convention. Should this be the case, the alleged infringement of the right to privacy on the part of public authority must be in accordance with the law which has to be accessible and sufficiently predictable, i.e. formulated with a high degree of accuracy, so that individuals can adjust their behaviour accordingly (cf. Malone v. UK, Amman v. Switzerland or Rotaru vs. Rumania). The level of accuracy required in national law, which can under no circumstances encompass all possibilities, depends to a large extend on the contents of the analysed text, area which is to be covered, and the number and status of persons for which it is intended [Hassan and Tchaouch v. Bulgaria (No. 30985/96, 39023/97) of 26 October, 2000]. The infringement of fundamental rights or freedoms, guaranteed under Article 8, paragraph 1 of the Convention, under review must in accordance with Article 8, paragraph 2 of the Convention be also essential to democratic society, follow the purpose approved by the Convention (e.g. protection of life or health of persons, national and public security, protection of rights and freedoms of others or morals, prevention of unrest and criminality or interest in economic welfare of a country), which must be relevant and given proper reasons for. The review can state that statutory provisions are in compliance with the Convention, if they in accordance with Article 13 of the Convention also provide appropriate protection against arbitrariness, and as a result of this sufficiently clearly define the scope and way of exercising powers granted to competent bodies (cf. Kruslin v. France or S. and Marper v. UK). In other words, acts constituting evident infringement of fundamental right to private life cannot be without any direct (preventive or ex-post) judicial control [cf. e.g. Camenzind v. Switzerland decision (No. 21353/93) of 16 December, 1997].

40. The European Court of Human Rights specified the above mentioned requirements for legal regulation allowing right to private life infringement in the above mentioned decisions, which review the admissibility of such infringement on the part of public authority in the form of wiretapping telephone conversation, secret surveillance, collecting data and information concerning private (personal) sphere of an individual. European Court of Human Rights emphasized that it is particularly important to define clear and detail rules concerning the scope and use of such measures, set minimum requirements for the time period, way of storing of information and data acquired, their use, access by third parties, and to anchor

procedures resulting in the protection of integrity and confidentiality of the data and also discarding of such data in a way so that individuals have sufficient guarantees against the risk of misuse and arbitrariness. The necessity to have such guarantees is even higher in case of protection of personal data subject to automatic processing, especially when such data is used for police purposes and at a time when available technology becomes more and more sophisticated. National law must primarily define that collected data are relevant indeed and not exaggerated in terms of the purpose for which they had been acquired, and further on, that they are stored in a form enabling the identification of persons during a certain time period not exceeding the necessary extent in order to meet the purpose, for which they had been acquired [cf. Preamble and Article 5 of the Convention on Data Protection and Principle 7 of the Council of Europe Committee of Ministers Recommendation No. R(87)15 of 17 September, 1987 concerning the regulation and use of personal data in the police sector, quoted according to Weber and Saravia decision v. Germany (No. 54934/00) of 29 June, 2006 or Liberty and others. v. UK (No. 58243/00) of 1 July, 2008].

VIII. The review

VIII. A) Data retention

41. As mentioned by the Constitutional Court above, contested provisions Section 97, subsection 3 and 4 became part of the Act No. 127/2005 Coll. based on Act No. 247/2008 Coll. amending the Act No. 127/2005 Coll., Act on Electronic Communications and on Amendment to Certain Related Acts (Electronic Communications Act) as amended. According to the explanatory report, this amendment has been adopted in order to implement "some articles" of the 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, which „have not been implemented into our law yet, or implemented only partially (because) the Data Retention Directive has already been transposed in the Czech Republic (…). The present legal regulation is in certain respects broader than regulation under Data Retention Directive." The Czech law regulates the issue of traffic and location data retention in a modified form since the adoption of the Electronic Communications Act No. 127/2005 Coll. itself effective from 1 May, 2005 and adoption of the contested Decree of the Ministry of Informatics No. 485/2005

Coll. on the Extend of Traffic and Location Data, the Time of Retention Thereof and the Form and Method of the Transmission Thereof to Bodies Authorised to Use such Data effective from 15 December, 2005. At that time, the EU was only preparing Data Retention Directive which was actually implemented in advance in the Czech Republic and the wording of contested provisions specifies the obligation to retain traffic and location data and provide such data upon request to authorised bodies without delay, as required by Data Retention Directive later on. The contested Decree of the Ministry of Informatics has however despite of this fact not been amended, resulting to the fact that the scope of retained data subject to the contested provisions thenceforth clearly exceeds the extent anticipated by the Data Retention Directive in question.

42. Pursuant to the contested provision Section 97, subsection 3, first and second sentence of the Electronic Communications Act, legal entities or natural persons providing public communication network or publicly available electronic communications service are obliged to retain traffic and location data generated or processed when providing public communications networks and electronic communication service, including data on abandoned calls, should this also be generated or processed and retained and recorded at the same time. Pursuant to Section 90 of the Electronic Communications Act, traffic data means "any data processed for the purposes of the transmission of a message via electronic communications network or for the billing thereof". Pursuant to Section 91 of the respective Act, 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 publicly available electronic communications service". More details and the scope of traffic and location data, the retention period and form and ways of transfer to authorised bodies shall be pursuant to the contested provision Section 97, subsection 4 specified in implementing provisions, which is the contested Decree No. 485/2005 Coll.

43. Providers of landline services and mobile communications are in particular obliged to retain virtually all available data on realized as well as (should this be recorded) abandoned calls (typically unanswered calls intended to alert the person dialled of something). The data relates in particular to the type of realized communication, incoming and dialled numbers, date and time of beginning and end of communication, indication of base station transmitting the call at the time of connection, prepaid phone card or public telephone booth identification, in case of mobile communication also data on the unique code identifying each mobile phone

used in the GSM network (IMEI), its location and movement, even if there is no communication under way (the phone is only switched on), number of credits for prepaid cards and the number recharged, information on mobile device and all inserted SIM cards etc. Even more information shall be retained pursuant to the contested provisions in connection with public packets-switched networks and their services, notably the Internet. Pursuant to contested legal provisions, when using such service, it is required to retain in particular data on network access (e.g. time, place, duration of connection, data on users and their user accounts, computer and accessed server identifier, IP address, full domain name, volume of data transferred etc.), further information related to electronic mail box access and transmission of electronic mail messages (in this case, virtually all information is retained with the exception of the contents itself, i.e. including address identification, volume of transmitted data etc.) and last but not least data on server and other services [e.g. URL addresses entered, type of request, data on chatting, user net, instant messaging (e.g. ICQ) and telephony IP including identification of parties involved in communication, time and service used (e.g. file transmission or transaction). Exceeding the frame of Data Retention Directive, in case of Internet connection and e-mail communications services, information on the volume of data, information on coding, method and status of service requests and realisation of service as well as information on SMS sent via Internet gates and other "special-interest identifiers" is monitored and retained. In case of telephony, exceeding the frame of the Data Retention Directive, the contested legal provisions require to retain data on prepaid card identification, public telephone booth, numbers or credit coupons and the numbers recharged, all SIM cards inserted into a mobile device.

44. Even thought the imposed obligation to retain traffic and location data does not cover the contents of individual messages (see Article 1, paragraph 2 of the Data Retention Directive and contested provision Section 97, subsection 3, sentence four), based on the combination of the above mentioned data on users, addressees, exact times, dates, locations and forms of telecommunication connections, if monitored over a longer period of time, detailed information on social or political profile, as well as personal preferences, inclinations and weaknesses of individuals can be compiled. The opinion of the proposer of the Act outlined in the statement of the Senate as summarized above, stating that "this does certainly not compare with wiretapping, let only because contents of particular telephone calls or e-mail messages are not retained", is completely incorrect, since barely based on such information, sufficient conclusions in term of the contents can be made falling within the private (personal) sphere of

an individual. Based on the data specified, it can be e.g. deducted with up to 90 % reliability, whom, how often and even at what time the particular individuals meet with, who are their closest acquaintances, friends or work colleagues, or which activities and at what time do they engage in [cf. study by the Massachusetts Institute of Technology (MIT), Relationship Inference, available at http://reality.media.mit.edu/dyads.php]. Location and traffic data collection and retention thus represent a serious infringement of the right to privacy and therefore, not only protection of the contents of the message conveyed via telephone communication or public networks communication itself, but related traffic and location data as well, have to fall under the scope of protection of fundamental right to respect for private life in the form of right to informational self-determination (pursuant to Article 10, paragraph 3 and Article 13 of the Charter).

VIII. B) Review of Contested Legal Provisions in Terms of Constitutional Requirements

45. The Constitutional Court therefore had to consider, whether contested legal provisions regulating the issue of universal and preventive collection and retention of the specified traffic and location data on electronic communication are in accordance with the requirements of the constitutional law as described above concerning legal regulation allowing infringement of fundamental right to privacy of individuals in the form of right to informational self-determination (pursuant to Article 10 paragraph 3 and Article 13 of the Charter). Moreover, given the intensity of such infringement, which is in this case more relevant due to the fact, that it applies to vast and unpredictable number of participants in a communication since this is a universal and preventive collection and retention of data, it was necessary to review the compliance with requirements mentioned above using the highest standards. The Constitutional Court came to the conclusion, that contested legal provisions do not meet the requirements of constitutional law by far, and that for several reasons.

46. Contested provisions of the Electronic Communications Act, Section 97, subsection 3, sentence three only vaguely and very indefinitely specify the obligation of legal entities or natural persons, that retain traffic and location data in the extent described above, to “make such data available upon request to the bodies entitled to request them on the basis of a special legal regulation” without any delay. Even thought the contested Decree specifies in Article 3 how to meet such obligation in individual cases in relation to entitled bodies, i.e. it describes relatively in detail the way of data transmitting, type of communication (electronic), format,

programs employed, codes etc., it is, in the opinion of the Constitutional Court, not clear neither from the wording of provisions of the Electronic Communications Act, Section 97, subsection 3, nor the explanatory report, which entitled bodies and which special legal regulation are particularly is meant. With regard to the wording of provisions of the Electronic Communications Act, Section 97, subsection 1, which lays down the obligation for legal entities or natural persons providing public communications network or providing electronic communications service accessible to general public to, at the requesting party´s expense, provide and secure interfaces at specified points of the network to connect terminal equipment for message tapping and recording, it can only be assumed, that the obligation to transmit retained traffic and location data applies to the same entitled bodies and special regulation addressed to the bodies involved in criminal proceedings, possibly pursuant to Criminal Code, Section 88a, Security Information Service, pursuant to Section 6 to 8a of the Act No. 154/194 Coll. on the Security Information Service as amended and Military intelligence pursuant to Act No. 289/2005 Coll. on Military Service, Section 9 and 10. Such definition of legal provisions allowing massive fundamental rights infringement does not meet the requirements for clarity with respect to law-abiding state (cf. paragraph 37).

47. At the same time, the purpose of transmitting traffic and location data to entitled bodies is not clearly and precisely defined, which makes it impossible to judge in how far are the contested provisions actually necessary (it is clear that the purpose can be met, i.e. purpose set in the Directive – see below). Whereas the quoted Data Retention Directive, Article 1, paragraph 1 clearly defines that it has been adopted in order to harmonise Member States´ provisions concerning the obligations of the providers of publicly available electronic communications services or public communications networks with respect to the retention of traffic and location data necessary to identify a participant or registered user with the aim to make such data “available for the purpose of investigation, detection and prosecution of serious crime” (even though it does not define these crimes in more detail), neither the contested provisions nor quoted provision of the Criminal Code, Section 88a, subsection 1 – regulating conditions of the use of retained data for the purposes of criminal proceedings – do encompass such limitations. Pursuant to this legal regulation, the legislator does thus not condition the option to use retained data in criminal proceedings by justified suspicion that a serious crime has been committed; at the same time, there is no regulation concerning the obligation of authorities involved in criminal proceeding to inform the (monitored) person thereof, not even ex-post, which does not meet the requirements resulting from the second

step of proportionality test, i.e. means selected must be necessary, since it is clear from the above stated, that the most regardful means in respect to fundamental right to informational self-determination has not been used.

48. The Constitutional Court does not consider such manner of (not) defining the spectrum of entitled public authorities as well as (not) defining the purpose for which they are entitled to request retained data, sufficient and predictable. Even though the use of retained data is pursuant to the quoted provision of the Criminal Code, Section 88a, paragraph 1 subject to judicial control in form of an permission issued by the presiding judge of the senate (in case of preparatory proceedings the judge), the legislator was primarily obliged to define more clearly and unambiguously circumstances and conditions of the use thereof as well as the scope of use in contested provisions or in the quoted provision of the Criminal Code, Section 88a, subsection 1, instead of using very vague definitions of terms of retained data use "on telecommunication that took place" in order to "clarify facts important for criminal proceeding". In particular, given the relevance and scope of the infringement of the right of individuals to privacy in form if right to informational self-determination (pursuant to Article 10, paragraph 2 and Article 13 of the Charter) represented by the use of such data, the legislator must limit the possibility to use retained data for purposes of criminal proceeding concerning very serious crimes only and only in case the pursued purpose cannot be reached otherwise. For that matter, this is the assumption not only of the quoted Data Retention Directive, but of the Provisions of the Criminal Code, Section 88, subsection 1 regulating conditions of wiretapping and telecommunications recording order ("should the criminal proceeding concern very serious crime"), however the respective provisions of Criminal Code, Section 88a, subsection 1 as a whole diverge without any reason from this (despite of legal opinions of the Constitutional Court inherent in mentioned judgments File No. II. ÚS 502/2000 or File No. IV. ÚS 78/01 – for both see above) and set regulation which clearly contradicts opinions of the Constitutional Court.

49. As it appears from the statistical data, the absence of proper legal regulation which would be in accordance with the Constitution in its meaning, results in practice in the fact, that the measure to request and use retained data (including data on abandoned calls not mentioned by the Criminal code at all) is used (overused) by authorities involved in criminal proceedings for purposes on investigating common, i.e. less serious criminal activity, as well. For example, according to the "Report on Security Situation in the Czech Republic in 2008", there

were 343 799 crimes in total identified in the territory of the Czech Republic, 127 906 crimes thereof were detected and in the same time period the number of requests for traffic and location data on the part of entitled public authorities reached the number of 131 560 (cf. EU Commission report "The Evaluation of Directive 2006/24/EC and National Measures to Combat Criminal Misuse and Anonymous Use of Electronic Data" whose authors requested official Czech data; reactions of representatives of the Czech Republic to questions of the interrogatory of 30 September, 2009 are available at http://www.dataretention2010.net/docs.jsp). In the following time period from January to October 2009 only, according to unofficial data, location and traffic data were requested in 121 839 cases (cf. Herczeg, J.: Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou, Bulletin advokacie No. 5/2010, p. 29).

50. The Constitutional Court also believes that legal regulation contested by the petitioners does not sufficiently enough or not at all define clear and detailed rules implying minimum requirements for the security of retained data, especially in the form of preventing third persons access, defining procedure resulting in protection of integrity and confidentiality of data and procedure of discarding data. Further critique concerning the contested regulation is that affected individuals do not have sufficient guarantees against the risk of data misuse and arbitrariness. The necessity to have such guarantees with respect to the considered issue of universal and preventive data collection and retention related to electronic communications however becomes even more important for an individual today, as enormous development and existence of new and more sophisticated information technologies, system and means of communication inevitably result in gradual shifting of the boundary between private and public sphere in favour of public sphere, since in virtual space of information technology and electronic communication (in the so-called cyberspace) thousands, even millions of data, facts and information are recorded, collected and virtually made accessible every minute, especially thanks to the development of the Internet and mobile communication, infringing the private (personal) sphere of every individual even though they have not intended to disclose it.

51. The Constitutional Court does certainly not consider the mere stipulation of obligation imposed on legal entities or natural persons to make sure that "the contents of messages shall not be retained together with specified data retained" (Electronic Communications Act, Section 97, subsection 3, sentence four), or obligation to "discard them after the elapse of the time, had they not been disclosed to authorities entitled to request them pursuant to special

legal provisions or should this Act specify otherwise (section 90)“ (Electronic Communications Act, Section 97, subsection 3, sentence six) to be clear, detailed and adequate enough guarantees. The mere definition of retention period of “no shorter than 6 month and no longer that 12 months”, given the lapse of this period influences the obligation to discard the data, can be deemed ambiguous and with respect to the scope and sensitive nature of retained data entirely insufficient. None of the obligations mentioned does describe rules or methods of meeting such rules in more detail, there is no strict definition of requirements concerning security of retained data, it is not entirely traceable how is the data handled neither on the part of legal entities or natural persons retaining traffic and location data, nor entitled public authorities after requesting the data; the way of discarding such data is not defined either. Further on, there is no definition of liability and respective sanctions in case of breach of such obligations, including missing establishment of the way how affected individuals can seek efficient protection against possible misuse, arbitrariness or non-fulfilment of defined obligations. The Electronic Communications Act (Section 87 and following provisions) envisions that The Office for Personal Data Protection (ÚOOÚ) will supervise whether “obligations are met when processing personal data”, which together with defined measures of its activities and control cannot be deemed as adequate and efficient means of protection of fundamental rights of affected individuals, since they do not exercise control over it themselves [cf. judgment File No. Pl. ÚS 15/01 of 31 October, 2001 (N 164/24 SbNU 201; 424/2001 Coll.) as appropriate]. The above mentioned acts present evident infringement of the fundamental right of individuals to privacy in form of right to informational self-determination (pursuant to Article 10, section 3 and Article 13 of the Charter) and they are thus – due to insufficient legal regulation which does not comply with the stated requirements of constitutional law – without any direct, not even ex-post control, judicial control in particular, which was deemed necessary even by the European Court of Human Rights in quoted decision Camenzind v. Switzerland.

52. Constitutional courts in other European countries dealing with the constitutionality of legal provisions implementing the Data Retention Directive in question, reached similar conclusions as well. For example, the Federal Constitutional Court of FRG considers in its judgment of 2 March, 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, the contested legal provision regulating the issue of preventive data retention (Vorratsdatenspeicherung) (pursuant to Section 113a, 113b of the Telecommunications Act (Telekommunikationsgesetz)) and the use thereof within criminal proceeding (pursuant to

Section 100g, subsection 1 of Criminal procedure Code (Strafprozessordnung)) unconstitutional due to contradiction with Article 10, Section 1 of the Basic Law for the Federal Republic of Germany (Grundgesetz), which guarantees inviolability of privacy of letters, post and telecommunication. The Federal Constitutional Court of FRG states that the contested legal provision is not in compliance with requirements resulting from the proportionality principle, which among others requires that the legal regulation of data retention reflects the particular seriousness of infringement of fundamental right of individuals. To be more specific, the contested legal regulation did not define the purpose of the use of such data sufficiently enough, it did not guarantee sufficient security thereof and furthermore did not sufficiently guarantee individuals adequate and effectual guarantees against misuse, in the form of judicial control in particular. The federal legislator was supposed to meet these requirements pursuant to Article 73, section 1, clause 7 of the Basic Law. The Rumanian Constitutional Court reached similar conclusions in its judgment of 8 October, 2009 (No. 1258), which considers the local legal regulation to be unconstitutional since it does not define the purpose of use of such measure sufficiently enough, its wording is too vague and does not set the powers and obligations of entitled public authorities in more detail and grant the affected individuals, due to absence of judicial control, sufficient guarantees against misuse (judgment in unofficial English translation available at http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html), further on, the Bulgarian Supreme Administrative Court in judgement of 11 December, 2008 (more information available at http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention) as well as Cyprus Supreme Court judgment of 1 February, 2011 (more information on http://www.edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus). The Constitutional Court learned that legal regulations implementing the Data Retention Directive in question are further on currently under review in Poland and Hungary. The necessity to ensure the strictest guarantees and measures of protection of fundamental rights of individuals as possible with respect to handling personal data from electronic communication has also been emphasised by the European Court of Justice in judgment in proceeding concerning preliminary question of 9 November, 2010 in joint cases Volker und Markus Schecke GbR GbR and Hartmut Eifert v. Land Hessen (C-92/09 a C-93/09).

53. Given the above stated, the Constitutional Court declares that contested provisions of Section 97, subsection 3 and 4 of the Electronic Communications Act No. 127/2005 Coll. and

on Amendment to Certain Related Acts (Electronic Communications Act), as amended, and contested Decree No. 485/2005 Coll. on the Extend of Traffic and Location Data, the Time of Retention Thereof and the Form and Method of the Transmission Thereof to Bodies Authorised to Use such Data cannot be deemed conform with the constitution, since they clearly violate the limits of constitutional law as explained above, because they do not meet requirements resulting from the principle of law-abiding state and are in collision with requirements concerning the infringement of fundamental right to privacy in the form of right to informational self-determination pursuant to Article 20, paragraph 3 and Article 13 of the Charter resulting from the principle of proportionality.

54. Apart from the above stated, the Constitutional Court deems it necessary to emphasise that described deficiencies, which led the Court to derogation of the contested legal regulation, are not even reflected in special legal regulations indirectly envisioned by contested provisions of Section 97, subsection 3 of the Electronic Communications Act. In particular, the above mentioned provisions of the Criminal Code, Section 88a, regulating requirements for the use of retained data on realized telecommunications traffic for purposes of criminal proceedings, do, in the opinion of the Constitutional Court, not respect the described limit of constitution law by far, and therefore they are deemed by the Constitutional Court unconstitutional as well. Nevertheless given the fact that the petitioners did not contest this provision in the proposal, the Constitutional Court believes, it is necessary to appeal to the legislator to consider, with regard to derogation of contested legal provisions, the amendment of the mentioned provisions of the Criminal Code, Section 88a, in order to reach conformity with the constitution.

VIII. C) *Obiter dictum*

55. Merely in the form of *obiter dicta*, the Constitutional Court declares that it is clearly aware of the fact that development of modern information technology and communication media goes hand in hand with new and more sophisticated ways of criminal activities that we need to deal with. However, the Constitutional Court doubts whether the instrument of universal and preventive traffic and location data retention on almost every electronic communication alone is a necessary and appropriate instrument in terms of the level of privacy infringement affecting enormous number of individuals involved in electronic communication.

Within the area of Europe, such opinion is by far not isolated since the Data Retention Directive itself has been heavily criticised from the very beginning of its existence by member states (e.g. governments of Ireland, the Netherlands, Austria or Sweden hesitated long or are still hesitating with its implementation, and moreover, the two last above mentioned countries do so despite a threat announced in public by the Commission to initiate European Court of Justice proceedings), as well as legislators in the European Parliament, the European Data Protection Supervisor (see conclusions of the data retention conference held by the Commission on 3 December, 2010 in Brussels, http://www.dataretention2010.net/docs.jsp) or the Data Protection Working Party set up pursuant to Article 29 of the Directive 95/46/EC (see its opinion available at http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm), or nongovernmental organisations (Statewatch, European Digital Rights or Arbeitskreis Vorratsdatenspeicherung – AK Vorrat among others). All the above mentioned demanded either the Data Retention Directive in question to be repealed in its full extend and the instrument of universal and preventive traffic and location data retention to be replaced by other more appropriate instruments (e.g. data freezing which makes it under certain fixed conditions possible to monitor and retain necessary and selected data of only a particular individual involved in communication determined in advance), or demanded the change thereof, in particular in the form if granting affected individuals satisfactory guarantees and means of protection and introducing stricter data retention security requirements preventing the threat of loss and misuse by third parties.

56. The Constitutional Court also has certain doubts resulting from the question whether the instrument of universal and preventive traffic and location data retention is an efficient instrument in terms of its original purpose (protection against security threats and prevention of particularly serious criminal activity), especially given the existence of so-called anonymous SIM cards, which do not fall within the anticipated scope of traffic and location data retained under the contested legal regulation and which – according to the Police of the Czech Republic – make up to 70 % of communication related to engagement in criminal activities (see "Česká policie chce zakázat anonymní předplacené karty, operátoři se brání" (The Police of the Czech Republic Seeks Ban on Pre-paid SIM Cards, Operators Fight Back), iDNES.cz, 18 March, 2010). In this context, reference can be made to the analysis of Germany´s Federal Criminal Police Office (Bundeskriminalamt) of 26 January, 2011, which based on comparison of statistic data on serious crimes committed within the territory of

Federal Republic of Germany during the time period prior to and after the adoption of the respective data retention legal regulation arrived at the conclusion that the use of instrument of universal and preventive traffic and location data retention had very limited impact on the reduction of the number of serious crimes committed as well as the respective detection rate (analysis and particular statistic data are available at http://www.vorratsdatenspeicherung.de/content/view/426/79/lang,de/). When overlooking crime statistics for the territory of the Czech Republic published by the Police of the Czech Republic, e.g. comparing statistical data for the time period between 2008 and 2010 (available at http://www.policie.cz/clanek/statisticke-prehledy-kriminality-650295.aspx), a similar conclusion can be drawn.

57. Despite this being mentioned at the end, the Constitutional Court deems necessary to express doubts concerning the desirability of entitling private persons (providers of Internet services and telephone and mobile communication, mobile operators and companies providing Internet access in particular) to retain all data concerning provided communication as well as customers to whom they provide services (i.e. even more data than they are legally obliged to retain pursuant to the contested legal regulations) and to use them unrestrictedly in order to collect their claims, develop business activities and use them for marketing purposes. The Constitutional Court considers this not to be desirable, in particular given that neither the Electronic Communications Act nor other legal regulations do not regulate such entitlement in more detail and depth, there is no strict definition of rights and duties, the scope of data retained, time period and retention method or more detailed specification of requirements regarding the security of such data and controlling mechanisms.

58. Taking into consideration the above stated, the Constitutional Court therefore decided pursuant to Section 70, subsection 1 of the Constitutional Court Act to repeal contested provisions of Section 97, Subsections 3 and 4 of the Act on Electronic Communications and on Amendment to Certain Related Acts (Electronic Communications Act) No. 127/2005 Coll., as amended, and contested Decree No. 485/2005 Coll. on the Extend of Traffic and Location Data, the Time of Retention Thereof and the Form and Method of the Transmission Thereof to Bodies Authorised to Use such Data as of the day of promulgation of this judgment in the Collection of Laws (Section 58, subsection 1 of the Constitutional Court Act).

59. Courts with general jurisdiction shall now consider each individual case in which data have already been requested in order to be used in criminal proceedings one by one – with respect to proportionality regarding privacy rights infringement. Courts shall consider primarily the seriousness of crime committed by the act against which criminal proceedings in which the requested data should be used are held.

Chairman of the Constitutional Court:
JUDr. Rychetský m. p.