# 2011/03/22 - PL. ÚS 24/10: DATA RETENTION IN TELECOMMUNICATIONS SERVICES

**HEADNOTES**

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

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

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

**On condition that the criminal law allows for exercising the public interest to prosecute criminal activity by means of robust tools the use of which results in serious limitations of the personal integrity and fundamental rights and freedoms of an individual, then when applied, constitutional law limits have to be respected.**

**Restrictions imposed on personal integrity and individual privacy (i.e. breaching**

**the respect towards them) may only be applied as an absolute exception, provided it is deemed necessary in a democratic society, unless it is possible to meet the purpose pursued by the public interest in any other way and if it is acceptable from the perspective of the legal existence and respecting effective and specific guarantees against arbitrariness. Essential presumptions of a due process require that the individual be provided with sufficient guarantees against the potential abuse of power by the public authorities.**

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

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

**CZECH REPUBLIC**
**CONSTITUTIONAL COURT**
**JUDGMENT**

**IN THE NAME OF THE REPUBLIC**

**JUDGMENT**

On March 22, 2011 the Constitutional Court panel consisting of Justices Stanislav Balík, František Duchoň, Vlasta Formánková, Vojen Güttler, Pavel Holländer, Vladimír Kůrka, Dagmar Lastovecká, Jan Musil, Jiří Nykodým, Pavel Rychetský, Miloslav Výborný and Eliška Wagnerová (judge-rapporteur) ruled on the petition filed by a group of Deputies of the Chamber of Deputies of the Parliament of the Czech Republic represented by Marek Benda, with their registered seat at Praha 1, Sněmovní 4, seeking to have the Section 97 Article 3 and 4 of the Act No. 127/2005 Coll., on Electronic Communications and Amendment of related Acts (Act on Electronic Communications) in their latest wording annulled and seeking to have 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 annulled, in the proceedings with the Chamber of Deputies of the Parliament of the Czech Republic and the Senate of the Parliament of the Czech Republic as parties to the proceedings, as follows:

Provision Section 97 para. 3 and 4 of Act No. 127/2005 Coll., on Electronic Communications and Amendment of related Acts (Act on Electronic Communications) in their latest wording and 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, are annulled as of the day on which this judgment is delivered within the Collection of Laws.

**REASONING**

**I.**
**Summary of the Petition**

1. The Group of 51 Deputies of the Chamber of Deputies of the Parliament of the Czech Republic sought in their petition filed with the Constitutional Court of the Czech Republic on March 26, 2010 to have the Section 97 Article 3 and 4 of the ActNo. 127/2005 Coll., on Electronic Communications and Amendment of related Acts (Act on Electronic Communications) in their latest wording (hereafter only as "the contested provisions) annulled and sought to have 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 (hereafter only as "the contested decree " or jointly hereafter only as "the contested legislation").

2. Although the petition complied with all formal requirements pursuant to Article 87 par. 1 Letter a) of the Constitution of the Czech Republic and to Section 64 para. 1 Letter b) of Act No. 182/1993 Coll., on the Constitutional Court in its latest wording (hereafter only as Constitutional Court Act) the Constitutional Court recognises the need to emphasise that the act of petition seeking annulment of law or its individual provisions pursuant to Articles 87 para. 1 Letter a) of the Constitution of the Czech Republic submitted by the group of Deputies of the Chamber of Deputies of the Parliament of the Czech Republic or by Senators pursuant to Section 64 para. 1 Letter b) of the Constitutional Court Act represents, inter alia, a representation of a constitutionally guaranteed principle of the protection of minorities (Article 6 of the Constitution of the Czech Republic) and primarily serves as one of the instruments of protection of parliamentary minority (the opposition) against a pertinent arbitrariness (or wilfulness) in decisions adopted by a parliamentary majority within the law-making process based on the principle of majority decision-making [see the report of the Venice Commission CDL-AD(2010)025 "Report on the Role of the Opposition in a Democratic Parliament" dated November 15, 2010 that includes the right enabling the parliamentary opposition to seek a constitutional review of majority decisions (laws) among the most fundamental rights conferred on parliamentary opposition.] In other words, a qualified submission to impartial and independent Constitutional Court frequently represents the final option of how the parliamentary minority may protect itself against pertinent arbitrariness in the decision-making of the parliamentary majority since the representatives of the parliamentary oppositions commonly represent a group outnumbered in the Parliament and thus have at their disposal no effective means through which such a majority decision (issuance of a normative legislative act) within the law-making process may be modified or reversed. Contrary to that the representatives of a parliamentary majority principally have such effective means at their disposal and should they be in doubt regarding rectitude, validity or even constitutionality of the decisions made (or having been made) they are not only entitled but directly obliged to make use of such means for the above mentioned purpose (see the oath pursuant to Article 23 par. 3 of the Constitution of the Czech Republic). The instrument of submission to the Constitutional Court seeking to have a law or its individual provisions annulled pursuant to Article 87 para. 1 Letter a) of the Constitution of the Czech Republic thus by no means serves as an instrument of obtaining a certain kind of “expert testimonial” or an expert report of the Constitutional Court on a decision adopted by a parliamentary majority nor as an instrumental application which represents a manifestation of political or even pre-election campaign transferred from the Parliament to the Constitutional Court. In this particular case the group of complainants not only consisted mainly of representatives of the political parties who at present participate and at the time of the submission participated in the exercise of government power and who had and continue to have the majority in the Chamber of Deputies of the Parliament of the Czech Republic required to amend the contested legislation, furthermore, and the Constitutional Court cannot omit a critical comment on this issue, most of them through their participation in the process of law-making by their affirmative (!) vote directly enabled adoption of the contested legislation. The Constitutional Court would in the future in such instances of its (mis)use have to be forced to dismiss submissions filed under such circumstances.

3. The complainants themselves summarised their objections by alleging that retention and use of traffic and location data on telecommunications services to the extent in which it is defined by the contested provisions and the contested decree represent an in-proportionate interference with the fundamental rights set forth by the Charter of Fundamental Rights and Freedoms (hereafter only as "the Charter") and in the Convention for the Protection of Fundamental Rights and Fundamental Freedoms (hereafter only as "the Charter), specifically interference with the fundamental rights conferred by Article 7 par. 1, Article 2 and 3 and Article 13 of the Charter and Article 8 of the Convention. Complainants maintain the above interference may further be perceived as a breach of essential requirements for a democratic state governed by the rule of law among which the principle of proportionality may be included pursuant to Article 4 Section 4 of the Charter. The complainants have supported their reasoning by the following arguments:

**I. A) Retention of Data on Communication as Interference with Private Life**

4. The content of the contested provisions is an imposition upon natural and legal persons providing the public telecommunications network or publicly accessible service of electronic communications (thus mainly the telephone operators and internet service providers) of a duty to retain the traffic and location data (tens of data) on entire telephone and facsimile communications, entire communications via e-mail and SMS, data on accession of websites and data regarding use of certain internet services specified by the contested decree for the period of 6 to 12 months. They are further obliged to provide the above specified data upon request to the authorised bodies. The complainants maintain that the above specified data undoubtedly fall within the scope of the protection pursuant to Article 8 of the Convention. They have relied on a number of judgments of the European Court for Human Rights (hereafter only as "the ECHR) and judgments of the Constitutional Court.

5. The complainants assume that interference with fundamental rights cannot be interpreted merely as an immediate interference (such as for instance familiarisation with the retained data) but also such measures of government bodies that represent a substantial threat to restricting the fundamental rights which may occur at any moment. Retention of traffic and location data cannot be but deemed to represent such a kind of interference since such data are continuously retained and are at the disposal of government bodies and such bodies may both request and use the data pursuant the applicable regulations. Retention of the above specified set of data is thus accompanied by a latent threat of further immediate interference of government bodies. Moreover, the fact that the traffic and location data are not retained by the state itself but that the use is made of private persons providing telecommunications services cannot be disregarded since the risk of potential misuse of the retained data by a great number of private persons actively involved in the area of telecommunications services is higher than in retention of such data by the state. One of the fundamental requirements of ECHR arrived at through interpretation of the condition of legitimate background for state interference with private life is the predictability and availability of such legitimate background. The reasons are represented by the legitimate and logical requirement of the individuals being in advance familiar with and aware of circumstances under which the state may exceptionally interfere with their private

lives and thus enabling the individuals to amend their actions accordingly so as to avoid such interference. The flat nature of retention of traffic and location data, however, restricts and/or prevents such an option.

6. The complainants assume that both the objectives and the probable and anticipated benefit resulting from the obligation to retain the traffic and location data is greatly disproportionate to the related interference with the fundamental rights of concerned individuals. Thus, pursuant to Article 8 par. 2 of the Convention they opted for the evaluation of the proportionality of the material measure in which they assessed the aspect of the significance and the extent of the interference with the fundamental rights of individuals, in the present case mainly with the right to privacy, they further assessed the aspect of legitimacy of the objective which is to be attained through restriction of fundamental rights and they assessed the aspect of the benefit of such interference. Last but not least they focused on the application of the measure in the view of threats represented thereof, mainly the threat of misuse of the retained data.

**I. B) Significance and Extent of the Interference with the Right to Privacy**

7. The complainants mainly pointed out that the introduction of the obligation to retain traffic and location data represents a substantial interference with the right to privacy since such data lend themselves to a broad number of options in which they may be used and in combination with other data may give rise to serious consequences affecting the private lives of the concerned persons. The obligation to maintain the traffic and location data to such an extent practically results in exclusion of the existence of uncontrolled and unmonitored telecommunications which must be considered as an exceptionally intense interference with the privacy of all persons using telecommunications means (telephony, use of Internet services) currently not only used for the purposes of communications among individuals but also affecting a wide spectrum of everyday activities (shopping, banking operations, education, medicine and others). The retained data may thus be used to deduce a wide range of other data (in a number of cases such data are extremely sensitive) on a concerned individual and their privacy. In a number of cases the identity of the addressee of a telephone call or e-mail may reveal a sensitive data on the sender (in the instances when the addressee might be a medical specialist), similarly the internet sites accessed may provide information on the attitudes, opinions and beliefs as well as on the medical condition and sexual orientation of the concerned person. Equally, a great amount of information may be obtained from location data on movements of mobile telephony (or rather the owner of such a device) mainly in combination with location of movements of other cellular phones (data on who encountered whom, at what time and at what location etc.). Based on the retained data a communication profile as well as movement profile of an individual may be elaborated to obtain not only data on the past activities of such an individual but also to accurately predict future activities of such an individual with a high probability which represents a significant interference with the right to protection of privacy and correspondence of individuals.

**I. C) Legitimacy of the Objective of Interference with Fundamental Rights**

9. The complainants further questioned in their petition the legitimacy of the objective to be attained by the contested legislation. The Government explanatory

report on Provision Section 97 of Act on Electronic Communications implies that the purpose of Provision Section 97 is to face the increasing risks and ensure the security and defence of the Czech Republic while not providing any more detailed explanation. The complainants assume that pursuant to Article 8 par. 2 of the Charter the interference with privacy is permissible in relation to combating criminal activities solely when applied to prevention of criminal activities. "Preventive general retention of telecommunications data not based upon an existence of a concrete and specific reason is mainly aimed at the past and may thus serve the purpose of clarification of criminal offences having been previously committed." (pg. 13). Thus the complainants assume that interference with privacy for the purposes of clarification of a previously committed criminal offence is contrary to Article 8 of the Charter. Furthermore the data are retained without any concrete and specific probable cause. Such a view adopted by the contested provisions implies that every individual is considered a suspect with no specific circumstances providing legitimate grounds for such suspicion and such an approach is not permissible in a state governed by the rule of law. The applicants equally pointed out (referring to specific foreign cases) the fact that evaluation of data on telecommunications services includes a threat of misinterpretation of such data and subsequently leads to suspicion and allegation directed against an innocent person. The identity of the person who engaged in communications might be mistaken for instance for the identity of the person who concluded the contract with the telephone services operator or with the Internet provider.

10. The complainants maintain that neither the entities submitting the Bill prior to the enactment of the Law nor the relevant bodies of state administration provided information concerning the number and kind of instances in which, prior to the enactment of the legislation which leads to extensive increase in the quantity of retained data and the possible access to such data, the investigation, detection and prosecution of serious criminal offences failed due to lack of access to the required data based on the fact that such data were no longer available. Equally, the fact whether the imposition of the duty to retain all data on telephone and electronic communications shall result in (or has already resulted in), compared to former provisions, a genuine improvement of investigation, in detection and prosecution of serious criminal offences as well in prevention of threats, in an increase of the percentage of resolved criminal offences and in a reduction of criminal activities is not established. Furthermore, the issue is how old the data requested by the relevant administrative and law enforcement bodies are and to what extent it is necessary to retain the traffic and location data for the period of six months and longer. Interference with privacy may paradoxically more frequently affect persons who do not participate in criminal activities of felonious and serious nature than persons who engage in such activities and thus are they increasingly interested in adopting anonymous ways of communication. The complainants assume that retention of data may assist in attaining the desired objectives to a lesser extent and in cases of lesser importance and thus a long term positive effect on the reduction of criminal activities cannot be anticipated in connection with use of telecommunications services.

**I. D) Threat of Misuse of Retained Data**

10. Complainants maintain that equally the risk of unlawful use and misuse of the retained data realistically exists since with such a great number of companies

providing telecommunications services (mainly mobile cellular communications and Internet communication) adequate security of the retained traffic and location data cannot be anticipated. It is thus necessary to test the realistic and technically available options of the use of such data. The complainants state the contested legislation fails to provide both the conditions under which the data is to be retained and the conditions for use of such data by the authorised bodies, moreover, it provides no guarantees of protection against misuse to individuals. The contested legislation thus aids extensive use of relevant databases both in the amount of data withdrawn from such databases and in the number of entities entitled to use such data as well as in the extent of purposes for which such data will be used. The complainants maintain that the threat of misuse of traffic and location data by third parties is genuine. The entities who might misuse such data frequently include employees of companies or government bodies that process the data as well as other persons (e.g. so-called hackers).

**I. E) Preliminary Questions Referred to the European Court of Justice**

11. The applicants conclude their petition by expressing their conviction that although the contested legislation represents national legislation to which criteria of constitutional order of the Czech Republic shall be applied it simultaneously represents an issue originating from community law, specifically from the transposition of the 2006/24/EC Directive of the European Parliament and the Council (hereafter only as "the Directive on data retention") into the legal order of the Czech Republic. The complainants proposed on the above mentioned grounds to the Constitutional Court of the Czech Republic for its consideration the possibility of referral to the European Court of Justice pursuant to Article 234 of the Treaty on European Community of a preliminary question regarding the validity or lack thereof of the Directive on data retention itself since a significant risk exists that the relevant Directive transposed into the Czech legal order through the contested provisions and the contested decree is contrary to European Community law.

## II. Summary of Opinions of Parties to the Proceedings

12. The Constitutional Court pursuant to Section 42 para. 4 a Section 69 of the Act on Constitutional Court sent the relevant petition seeking to have the contested provisions and the contested decree revoked to the Chamber of Deputies and the Senate of the Chamber of Deputies of the Parliament of the Czech Republic as well as to the Public Defender of Rights.

13. The Chamber of Deputies of the Parliament of the Czech Republic represented by its Chairman, Ing. M. Vlček in its opinion dated April 26, 2010 described in detail the procedure of the enactment of the Bill by which the Act on Electronic Communications No. 127/2005 Coll. is amended and on amendment of certain related Laws (Act on Electronic Communications) in its latest wording on the basis of which the contested provisions were established as part of the Act No. 127/2005 Coll. on Electronic Communications (for more detail see part VI. of this Judgment). It further noted regarding the content of the government proposal that in its explanatory report the government had expressly stated the proposed Bill was in compliance with the constitutional order and the legal order of the Czech Republic

and is not contrary to any of the international treaties the Czech Republic is bound by. The Chamber of Deputies of the Parliament of the Czech Republic perceived and approached the Bill on the grounds of the above. It is thus upon the Constitutional Court to assess the constitutionality of the contested provisions.

14. The Senate of the Parliament (Senát Parlamentu) of the Czech Republic represented by its Chairman MUDr. P. Sobotka in its opinion dated April 28, 2010 after having extensively summarised the argumentation of the applicants contained in the assessed petition described the procedure of enactment of the relevant Bill by the Senate (for more detail see part IV of this Judgment). It further noted, regarding the hearing of the Bill, that the Bill was introduced to the Committee on Economy, Agriculture and Transport, as well as to the Standing Senate Commission on Media and later to the Plenary Session of the Senate as another amendment in response to the obligation of the Czech Republic to transpose the relevant Directive of EC within our legal order. On the matter of obligation of the telecommunications operators, internet providers and other entities active in the field of electronic communications to retain location and traffic data for the minimum period of 6 months the submitter emphasised that "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." The Senate accepted the above fact in its hearing of the concerned Bill and upon recommendation of the Committee and the Standing Senate Commission on Media approved the Bill in the wording accepted by the Chamber of Deputies. It is thus upon the Constitutional Court to assess the petition seeking to have the concerned provisions of Act on Electronic Communications revoked and issue a final decision.

15. JUDr. Otakar Motejl, the Public Defender of Rights in his opinion dated April 12, 2010 stated that after consideration of the submitted petition he does not endorse the arguments of the petition and thus waives his right to participate in the proceedings on annulment of the contested decree before the Constitutional Court.

**III.**
**Refrainment from Oral Hearing**

16. Pursuant to provisions Section 44 para. 2 of Act on the Constitutional Court the Constitutional Court may upon consent of the parties to the proceedings refrain from an oral hearing if further clarification of the matter cannot be expected from such a hearing. Pursuant to the above provision the Constitutional Court requested an opinion from the parties to the proceedings regarding their consent to refrain from an oral hearing. The complainants and the Senate of the Chamber of Deputies of the Parliament of the Czech Republic granted their consent. The Chamber of Deputies of the Parliament of the Czech Republic failed to respond within the time constraint determined by the Court. Thus in the present case the Court was able to refrain from listing an oral hearing in the present matter.

**IV.**
**Constitutional Conformity of Procedure by which the Contested Provisions of Law were Enacted and Statutory Conditions of the Adopted Decree**

17. In proceedings on annulment of statutes pursuant to Article 87 par. 1 Letter a) of the Constitution of the Czech Republic pursuant to provision Section 68 par. 2 of the Act on the Constitutional Court, the Constitutional Court is to primarily test whether the concerned Act was enacted and issued in the constitutionally prescribed manner [regarding the algorithm of the review in proceedings on control over statutory norms see leg 61 of the Constitutional Court Judgment Pl. ÚS 77/06 dated February 15, 2007 (N 30/44 SbNU 349; 37/2007 Coll.)]. In the instances of statutory instruments, mainly the ministerial decrees, the Constitutional Court pursuant to Section 68 par. 2 of the Act on Constitutional Court assesses whether they were enacted and published within the authority and scope defined by the Constitution of the Czech Republic (Article 79 par. 3 of the Constitution of the Czech Republic), it is whether they were not published "ultra vires".

18. The Constitutional Court found, based on the opinions of both of the Chambers of the Parliament of the Czech Republic, the attached enclosures and documents accessible via electronic channels (resolutions and publications accessible in the digital library and on the web sites of the Chamber of Deputies and the Senate and on www.psp.cz a www.senat.cz) as follows: The contested provisions Section 97 para. 3 and 4 were included within the Act No. 127/2005 Coll., on Electronic Communications pursuant to Act No. 247/2008 Coll., by which the Act No. 127/2005 Coll., on Electronic Communications and on Amendment on Certain Related Acts (Act on Electronic Communications) was amended. The Bill of the above Act was submitted to the Chamber of Deputies by the Government of the Czech Republic on January 16, 2008 while the hearing of the Bill was proposed in such a manner as to enable the Chamber of Deputies to grant its approval within the First Reading. The Deputies were sent the Bill on January 18, 2008 as an official document of the Chamber of Deputies No. 398/0 - Amendment of the Act on Electronic Communications - EU. In the first reading on January 30, 2008 at the 27th meeting the 1. Chamber of Deputies failed to pass the Bill within the hearing in a manner requested for the approval of the Bill in the First Reading. The Bill was subsequently referred to the Economy Committee, Legislative and Constitutional Committee and the Security Committee (resolution No. 593). The relevant committees heard and discussed the Bill and their resolutions as well as the proposed amendments were delivered to the Deputies as communications notices No. 398/1, 398/2 and 398/3. The amendments proposed by the Security Committee were the only ones related to the contested provision Section 97 para. 3 (the third and the fifth sentence). The second reading of the Bill was conducted at the 28th assembly of the Chamber of Deputies on March 20, and 25, 2008. The Bill underwent a general and detailed debate in the course of which the proposed amendments were submitted by individual Deputies (proposed amendment by Z. Bebarová-Rujbrová, by K. Jacques and J. Klas) regarding the contested provisions (section 97 para. 3 the third and the fifth sentence and section 97 para. 4). The submitted proposals of amendments were processed as notice 398/4, sent to the Deputies on March 25, 2008. The third reading was conducted on April 23, 2008 at

the 30th assembly of the Chamber of Deputies. The amendments proposed to the contested provisions section 97 para. 3 and 4 were not adopted. The Bill of the Act was enacted in the wording of further adopted amendments (resolution No. 736) upon consent by the Chamber of Deputies when 89 of the 176 Deputies present voted in favour of the Bill, 21 voted against the Bill and 66 abstained from the vote. (vote No.44).

19. The Chamber of Deputies passed the relevant Bill on to the Senate on May 19, 2008. The Organisation Committee of the Senate determined the Bill as the Senate Communication Document No. 247 to be discussed by the Committee for Economy, Agriculture and Transport. The Bill was further discussed by the Standing Senate Commission on Media. On its meeting on May 28, 2008 the Committee adopted a resolution No. 270 in which it recommended to the Senate to approve the Bill. The Standing Senate Commission on Media equally recommended that the Senate approve the Bill (resolution No. 22 of June 4, 2008). The Senate discussed the Bill on June 5, 2008 at its 14th meeting (6th term of the Senate) and adopted Resolution No. 402 on the Bill by which it approved the Bill in the wording referred to the Senate by the Chamber of Deputies. 38 Senators of the 52 present voted in favour of the Resolution, 2 voted against and 12 abstained from the vote (vote No. 29).

20. The Act was delivered to the President of the Czech Republic for signature on June 11, 2008 and the President signed the Act on June 25, 2008. The approved Act was delivered to the Prime Minister of the Czech Republic on June 30, 2008 for signature. The Act was published on July 4, 2008 in the Collection of Laws in Section 78 under No. 247/2008 Coll. coming into force on September 1, 2008.

21. The contested decree No. 485/2005 Coll., on the Extent of Traffic and Location Data, Period of Time for which such Data are Retained and the Manner in which they are Submitted to Bodies Authorised to Use the Data was published by the Ministry of Informatics of the Czech Republic. The authority of the ministries to issue legal regulations on implementation of law is conferred by Article 79 par. 3 of the Constitution of the Czech Republic. It is, however, materially conditioned by the existence of an express authorisation and its restrictions. In this particular case the contested section 97 of the para. 4 of Act No. 127/2005 Coll., on Electronic Communications, represents such a type of authorisation. The decree was signed by the Minister of Informatics and duly published in part 169 under the number 458/2005 of the Collection of Laws with the date of enforceability identical with the date of its publication, that is December 15, 2005.

22. The Constitutional Court finds that both the Act no. 247/2008 Coll., by which the contested provisions were inserted into Act No.. 127/2005 Coll., on Electronic Communications and the contested decree No. 485/2005 Coll., were enacted constitutionally.

## V.
## Wording of the Contested Provisions and the Contested Decree

23. The contested provisions section 97 para. 3 and 4 of Act No. 127/2005 Coll., on

Electronic Communications and Amendment of related Acts (Act on Electronic Communications, in its latest wording read as follows:

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 37b). 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.

_____
37b) The Directive 2006/24/EC of the European Parliament and of the Council of March 15, 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.

24. The contested decree No. 485/2005 Coll., on the Extent of Traffic and Location Data, the Period of Time for which they are Retained and the Form and Manner in which they are Submitted to the Bodies Authorised to Use them reads as follows:

485/2005 Coll.
DECREE
dated December 7, 2005

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

The Ministry of Informatics in cooperation with the Ministry of Interior

shall pursuant to Section 150 para. 3 of Act No. 127/2005 Coll., on Electronic Communications and Amendment of related Acts (Act on Electronic Communications) in the wording of Act No. 290/2005 Coll. and Act No. 361/2005 Coll, (hereafter only as “the Act”) set forth for implementation of Section 97 para. 3 of the Act:

Section 1
For the purposes of this Decree the following terms are understood to mean as follows:
a) BTS station as the base station of public mobile telephone network,

b) StartBTS station as the base station of a public mobile telephone network within which a subscriber is allocated upon commencement of the communication,

c) StopBTS station as the base station of a public mobile telephone network within which a subscriber is allocated upon cessation of the communication

d) IMEI number as the international identification number of the mobile telephone device,

e) MSISDN number as the subscriber’s number within the public mobile telephone network,

f) IMSI number as an international public mobile telephone network subscriber identity,

g) the destination as determination of foreign network operator,

h) URI identifier as uniformed resource identifier,

i) code of the legal entities or natural persons providing the public communications network or providing publicly available services of electronic communications as the serial number of the licence in the register of business entities pursuant to Section 14 of the Act.

Section 2
Extent of the Retained Traffic and Location Data
(1) A legal entities or natural person providing public communications network or providing publicly available services of electronic communications (hereafter only as "the provider") provides the traffic and location data defined by this Decree (here after only as “the data”) to the body authorised to request such data (hereafter only as the authorised body).

(2) In electronic communications networks with circuit switching and fixed connection the following data are retained:
a) data on occurred communication specifying the type of communications, telephone numbers of the caller subscriber and the called subscriber or the identifier of public telephone telephone card, date and time of commencement of communication, length of communication and if appropriate data on the state of communication,

b) data on all public telephone including their telephone numbers, registration number, geographical coordinates and express description of their location.

(3) In public mobile telephone electronic communications the following data is retained:
a) data on occurred communication specifying the type of communication, telephone numbers of the caller subscriber and the called subscriber, date and time of commencement of communication, length of communication, IMEI number, StartBTS station number, StopBTS station number if appropriate, the destination and additional information,

b) data on mutual relations among MSISDN and IMEI numbers jointly used in networks, BTS station, IMEI number identification, enabling calls without the use of a SIM card to the "112" emergency number, IP addresses of terminals enabling dispatch of SMS messages via an Internet network, date and time of credit recharge in prepaid services, numbers of recharge vouchers for a specific telephone number of subscriber and the telephone number of subscriber for a specific recharge voucher,

c) data on all BTS stations including their number, geographical coordinates, azimuth angle of aerial routing and express description of BTS station location.

(4) In the case of electronic communications networks with packet switching, the data on communication are stored as follows:
a) In the case of services accessing a network: connection type, user account identifier, service user equipment identifier, date and time of connection opening, date and time of connection closing, interest identifiers (e.g. IP address or port number), event status (e.g. success, failure, or regular or extraordinary connection closing), and volume of transferred data (downloaded and uploaded);

b) In case of services accessing electronic mail boxes: user equipment identifier, user account, message identifier on the mail server, date and time of communication opening, sender's electronic mail address, receivers' electronic mail addresses, electronic mail protocol identifier, volume of transferred data, and information on using encrypted communication;

c) In the case of services of transferring electronic mail messages: user equipment identifier, electronic mail server identifier, date and time of communication opening, sender's electronic mail address, receivers' electronic mail addresses, electronic mail protocol identifier, volume of transferred data, and information on using encrypted communication;

d) In the case of server services: user equipment identifier, user account identifier, data and time of request for service, all server identifiers (in particular, IP address or full domain name FQDN), URI or service type identifiers requested, additional URI or service identifiers parameters, used services, volume of transferred data, and method and status of request for service;

e) In the case of other electronic communications services (such as chat rooms,

UseNet, instant messaging, and IP telephony in particular): all communicating parties' identifiers, transfer protocol, data and time of communication opening, date and time of communication closing, used services, and volume of transferred data.

Section 3
Manner of handing over retained data
(1) The competent public authority shall apply for provision of the retained data by means of a specific contact point . The data pursuant to Section 2, para. 3, letter c) shall be handed over on a monthly basis in its current state as to the handover date.

(2) Preferentially, communication between the contact points of the operator and the competent authority shall take place in a manner allowing remote access. If possible, applications and data shall be submitted in the electronic form of data files. Only generally available technologies and communication protocols shall be used for the communication purposes between the individual contact points so that the solution is not associated with a particular producer or supplier.

(3) Unless the manner allowing remote access cannot be used for the communication purpose, or provided that using remote access is not efficient, the application or data may be submitted in a documentary form or in the form of data files on a portable medium.

(4) For the purposes of verifying the authenticity of the application and submitted data the following shall be used:
a) Certified electronic signature based on a qualified certificate issued by an officially accredited provider of certification services; the format of a cryptographic standard with public key PKCS#7 shall be used for the purposes of signature creation and verification;

b) A covering letter in the documentary form containing the application reference or serial number, file name, date, time and manner of submission, and possibly also a check sum or standard file hash (e.g. SHA-1) and the authorised person's signature;

c) A letter in the documentary form containing the reference number and the authorised person's signature, or

d) In case of applications and data already submitted in electronic form and covering a certain period, usually one week, where no other authentication means has been used, a letter in the documentary form containing the reference number and the authorised person's signature, sent post facto.

(5) Data on communication taking place before a certain identifier for a certain period of time shall be submitted by the provider to the competent authority as:

a) records of fixed line communications in the case of data pursuant to Section 2, para. 2, letter a);
b) records of mobile communications in the case of data pursuant to Section 2,

para. 3, letter a);
c) records of data communication in the case of data pursuant to Section 2, para. 4.

(6) Records in compliance with Paragraph 5 shall be submitted to the competent authority in the form of a structured text file, preferentially coded according to character sets CP-1250, UTF-8 or ISO 8859-2. The file shall be processed separately for every individual telephone number or any other identifier included in the application. The names of files for submission shall be structured following the convention included in the Annex.

(7) The file shall be introduced with a uniform header and shall be of a fixed structure defined for a specific network or service type or application type. Individual lines in the file shall be arranged chronologically, unless stated otherwise in the application. The records in compliance with Paragraph 5 shall be closed with the word “End” on the last line.

(8) On every line, individual data shall be separated with a semi-colon (code 0059 of the character set) or tabulator (code 0009 of the character set); the last entry shall be closed with the CRLF character (code 0013 and 0010 of the character set). On condition that some data are not requested or may not be demonstrably ascertainable given the specific technology, its place within the structure shall remain empty.

(9) In the case of entries containing more values, individual values shall be separated by character "|" (code 0166 of the character set). On condition that the submitted data contain a character equal to any of the afore-mentioned separators or character " (code 0092 of the character set), it shall be preceded with character " (e.g. "", "", or "\").

(10) In well-reasoned cases and following the approval of the competent authority and the operator, it is possible to use a file format, name and structure different from the description included in paragraphs 6 to 9.

Section 4
Length of data retention
(1) The data shall be retained for the period of 6 months, unless stated otherwise in paragraph 2.
(2) The data referred to in Part 3, sections 3.3.4.5 and 3.3.4.6 of the Annex shall be retained for the period of 3 months.

Section 5
Effectiveness
The Decree hereof shall come into effect upon its publication date, with the exception of Section 4, para 2. and Part 2 of the Annex, both coming into force on 1 December 2006.

Minister:
Ing. Bérová (signature)
---

1) Section 11 of Act No. 227/2000 Coll., on Electronic Signature, as amended.

## VI.
## Reference for a Preliminary Ruling

25. Above all, the Constitutional Court had to assess the petition filed by the complainants to submit to the European Court of Justice, in compliance with Article 234 of the EC Treaty, a reference for a preliminary ruling concerning the (in)validity of the Data Retention Directive, since there is a significant risk that the Data Retention Directive, on its own, which has been implemented into the Czech legal system by means of the contested provisions and contested Decree, is inconsistent with the EC law. . In this respect, the Constitutional Court points out that even after the accession of the Czech Republic to the EU (since 1 May 2004), the norms and standards of Czech constitutional order have remained the reference framework for review performed by the Constitutional Court, since the role of the Constitutional Court lies in protecting constitutionality (Article 83 of the Constitution of the Czech Republic) in both aspects, i.e. the protection of the objective constitutional law, and subjective (i.e. fundamental) rights. The Community law is not part of the constitutional order, and therefore the Constitutional Court is not competent to interpret it. Despite this, the Constitutional Court cannot entirely overlook the impact of the Community law on the formation, application and interpretation of national law, all the more so in the field of law where the creation, operation and aim of its provisions is bound up with community law [cf. the relevant Judgments of the Constitutional Court file reference Pl. ÚS 50/04 issued on 8 March 2006 (N 50/40 SbNU 443; 154/2006 Sb.), file reference Pl. ÚS 36/05 issued on 16 January 2007 (N 8/44 SbNU 83; 57/2007 Sb.), or file reference II. ÚS 1009/08 issued on 8 January 2009 (N 6/52 SbNU 57)]. The content of the Data Retention Directive, however, provides the Czech Republic with sufficient space to implement it in conformity with the constitutional order, since its individual provisions in fact only define the obligation to retain data. For the transposition purposes the objective defined by the corresponding Directive must be met, yet in case of specific laws and bye-laws concerning data retention and handling, including security measures and misuse prevention, it is necessary to follow the constitutional standard based on the Czech constitutional order as interpreted by the Constitutional Court. The reason for this is the fact that the particular implementation form, i.e. the challenged provisions of the relevant laws and bye-laws, is an expression of the will of the Czech legislature or, which may vary to some extent as far as the choice of relevant means is concerned, while observing the Directive's objective, yet when making such choice, the legislature was at the same time bound to the constitutional order.

## VII.
## Framework of Reference for Assessment of the Petition

### VII. A) Right to respect of private life and right to informational self-determination

26. Section 1, para. 1 of the Constitution of the Czech Republic provides for a normative principle of a democratic rule of law state. The notion of the rule of law

is essentially based and conditioned by respecting the fundamental rights and freedoms of an individual which is, as an attribute of the selected rule of law state expressly stipulated in the constitutional provision referred to above. This constitutional provision serves as a basis for the materially perceived legal statehood, characterised by the respect of the state authorities to the individual's free (autonomous) sphere delineated by fundamental rights and freedoms, while the state authorities essentially do not interfere with this sphere, or possibly interventions only take place in 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.

27. The notion of privacy tends to be commonly associated with Western culture, and even more precisely, with an Anglo-American cultural idea embedded in the political philosophy of liberalism. Obviously, it is not a generally shared notion, both with respect to the emphasis on the importance of privacy, and to the extent of what should fall within the protection of privacy. Different cultures have developed various ideas as to the scope of privacy to which individuals are entitled, and in what contexts. Yet even in 1928, Judge Brandeis assessed privacy in his subsequently often quoted dissenting opinion (in relation to the case of Olmstead v. United States 438, 478, 1928) as follows: "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness.. [...] They conferred, as against the Government, the right to be "let alone" - the most comprehensive or most extensive of rights, and the right most valued by civilized men.." And therefore, the right of privacy, previously not expressly stipulated, has developed over time into one of the essential structural elements of the American Constitution, providing the individual with autonomy; yet its exercise has been repetitively battled for within the US Supreme Court.

28. Apart from the request to respect one's own life, physical, psychological and spiritual integrity, personal freedom, and possession, the request to respect the autonomous life setup has become a core human right claim for individual autonomy, which has a formative importance to European national catalogues of human (fundamental) rights, as well as to their subsequent regional and universal pendants. Yet even original European national catalogues of fundamental rights did not expressly include the right of privacy or private life itself, which may be substantiated by wordings of national Constitutions as approved in the 1940s or 1950s (e.g. the Constitution of the Federal Republic of Germany, not to mention the one of Austria, the Constitution of Denmark, Finland, as well as France, Ireland, Italy, and other countries). The requests to respect privacy and its protection are actually closely related to the development of technical and technological possibilities, obviously increasing the potential of the state to threaten freedom.

29. As the Constitutional Court held in its judgment (file reference II. ÚS 2048/09 issued on 2 November 2009, (available in the electronic decision database on http://nalus.usoud.cz): "In liberal democratic states, the fundamental right of undisturbed private life (Article 10, para. 2 of the Charter) enjoys very specific respect and protection." The primary function of the right of respecting private life

is to provide space for development and self-realisation of the individual personality. Apart from the traditional definition of privacy in its space dimension (protection of the home in a broader sense) and, in connection with the autonomous existence and public authority, undisturbed creation of social relationships (in a marriage, family or society), the right to respecting private life also includes the guarantee of self-determination in the sense of primary decision-making of an individual about themselves. In other words, the right to privacy also guarantees the right of an individual to decide, at their own discretion, whether and to what extent, how and under what circumstances the facts and information concerning their personal privacy should be made accessible to other entities. This aspect of the right to privacy takes the form of the right to informational self-determination, expressly guaranteed in Article 10, para. 3 of the Charter [cf. the Judgments of the Constitutional Court, file reference IV. ÚS 23/05 issued on 17 July 2007 (N 111/46 SbNU 41) or file reference I. ÚS 705/06 issued on 1 December 2008 (N 207/51 SbNU 577), or possibly the Decision of the Federal Constitutional Court of Germany issued on 15 December 1983, BVerfGE 65, 1 (Volkszählungsurteil) or issued on 4 April 2006, BVerfGE 115, 320 (Rasterfahndungurteil II)].

30. In the quoted Decision BVerfGE 65, 1, the Federal Constitutional Court of Germany, when asked to assess the constitutionality of the provisions concerning gathering and storing data for the purposes of a census (Volkszählung) stated, among other things, that in modern society, characterised also by a substantial increase of information and data, the protection of an individual against uncontrolled gathering, storing, using and publishing data concerning their personality and privacy must be provided within a more general right to privacy, guaranteed by the Constitution. Unless the individual enjoys the guarantee of controlling and checking the content and extent of information and data provided by them to be published, stored or used for other than the original purposes; unless they are provided with the possibility to recognise and assess the credibility of their potential communication partner and adapt their action accordingly, then their rights and freedoms are unavoidably restricted or even suppressed, and consequently, it is no longer possible to perceive such a society as free and democratic. The right to informational self-determination (informationelle Selbstbestimmung) is thus a necessary condition not only for free development and self-realisation of an individual, but also for establishing free and democratic communication rules. To put it simply, under the circumstance of an omniscient and omnipresent state and public authority, the freedom of expression, the right of privacy and the right of the free choice of behaviour and acting become virtually non-existent and illusionary.

31. The Charter does not guarantee the right to respect for private life in a single all-encompassing article (as is the case of Article 8 of the Convention). On the contrary, the protection of the individual private sphere in the Charter is distributed and complemented with other aspects of the right to privacy declared in various sections of the Charter (e.g. Article 7 para. 1, Article 10, Article 12, and Article 13 of the Charter). Similarly, the right itself to informational self-determination may be derived from Article 10, para. 3 of the Charter, providing the individual with the guarantee of the right to protection against unauthorised gathering, publishing or any other misuse of information concerning their person, in association with Article 13 of the Charter, protecting the confidentiality of letters

or the confidentiality of other papers or records, whether privately kept or sent by post or transferred by telephone, telegraph or any other similar equipments or means. Nevertheless, the "fragmentation" of the legal provisions concerning the aspects of the individual's privacy cannot be overestimated, while the list contained in the Charter and concerning what needs to be ranked under the "umbrella" of the right to privacy or private life cannot be deemed exhaustive and ultimate. When interpreting the individual fundamental rights depicting the right to privacy in its various dimensions as stipulated in the Charter, it is necessary to respect the purpose of the generally understood and dynamically developing right to privacy as a whole, i.e. it is necessary to consider the right to private life in its integrity at the given time. For this reason, the right to informational self-determination, guaranteed in Article 10, para. 3 and Article 13 of the Charter, must also be interpreted particularly in connection with the rights guaranteed in Articles 7, 8, 10, and 12 of the Charter. Due to its character and importance, the right to informational self-determination thus falls within the fundamental human rights and freedoms, since it contributes to establishing, together with personal freedom, freedom in the spatial dimension (dwelling), communication freedom, and certainly other constitutionally guaranteed fundamental rights, the personal sphere of the individual, whose individual integrity, as an absolutely essential condition of dignified existence of the individual and the development of human life as a whole, must be respected and protected in a consistent manner. For this reason, the respect to and the protection of this sphere is justly guaranteed by the constitutional order , since - when considered from a relatively different perspective - it is an expression of respect to the human and citizen rights and freedoms (Article 1 of the Constitution of the Czech Republic).

32. The established case law of the Constitutional Court, mainly in relation to the issues of telephone call interception, clearly indicates that the protection of the right to the respect of private life taking the form of the right to informational self-determination in the sense of Article 10, para. 3 and Article 13 of the Charter applies to not only the content of messages transferred over the telephone, but also to the data on the numbers called, date and time of the telephone call, its length, and in case of mobile telephony, to the base stations allowing the telephone call connection [cf. e.g. the Judgment file reference II. ÚS 502/2000 issued on 22 January 2001 (N 11/21 SbNU 83) - "The privacy of every individual is worthy of fundamental (constitutional) protection not only in relation as to the content of the transferred messages but also as to the afore-mentioned data". It may thus be stated that Article 13 of the Charter also provides for the protection of confidentiality of numbers call and other related data, such as date and time of the phone call, its length, and in case of mobile telephony, the identification of the base stations allowing the telephone call connection. [...] Such data represent an inseparable part of communication taking place over the telephone"; or similar judgments file reference IV. ÚS 78/01 issued on 27 August 2001 (N 123/23 SbNU 197), file reference I. ÚS 191/05 issued on 13 September 2006 (N 161/42 SbNU 327), or file reference II. ÚS 789/06 issued on 27 September 2007 (N 150/46 SbNU 489)].

33. In the quoted Judgments, the Constitutional Court also followed the case law of the ECHR [particularly the judgment issued in the case of Malone v. UK (no. 8691/79 issued on 2 August 1984)], which - following Article 8 of the Convention,

guaranteeing the right to respect for private and family life, as well as the home and correspondence, also concluded the right to informational self-determination, emphasising on a number of occasions that data collection and retention concerning an individual's private life fall within the scope of Article 8 of the Convention, since the term "private life" must not be interpreted in a restrictive manner. This facet of the right to privacy thus also consumes the right to protection against monitoring, surveillance and pursuit performed by public authorities, also in public areas and places accessible to the public. Furthermore, there is no fundamental reason allowing the exclusion of professional, business or social activities from the term of private life [cf. the Judgment in the case of Niemietz v. Germany (no. 13710/88) issued on 16 December 1992]. As stated by the ECHR, such extensive interpretation of the term of "private life" is in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (drawn up by the Council of Europe on 28 January 1981 and coming into force in the Czech Republic from 1 November 2001, published under No. 115/2001 of the Collection of International Treaties), whose objective 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), whereas it is defined as any information relating to an identified or identifiable individual" (Article 2). [cf. the Judgment in the case of Amman v. Switzerland (no. 27798/95) issued on 16 February 2000 and the appropriate quoted case law].

34. In its judgments relating to the respect for private life pursuant to Article 8 of the Convention, the ECHR defined as infringement of individual privacy, among others, infringements in the form of monitoring data, the content of correspondence and telephone call interception [cf. the Judgment in the case of Klass and others v. Germany (no. 5029/71) issued on 6 September 1978, the Judgment in the case of Leander v. Sweden (no. 9248/81) issued on 26 March 1987, the Judgment in the case of Kruslin v. France (no.11801/85) issued on 24 April 1990, or the Judgment in the case of Kopp v. Switzerland (no. 23224/94) issued on 25 March 1998], monitoring the telephone numbers of the persons making a telephone call [cf. the Judgment in the case of P. G. and J. H. v. UK (no. 44787/98) issued on 25 September 2001], collecting data on telephone connection (compared to the Judgment in the case of Amman v. Switzerland, referred to above), or storing the data on individuals' DNA in defendants' databases [cf. the Judgment in the case of S. and Marper v. UK (no. 30562/04 and 30566/04) issued on 4 December 2008]. In the Judgment in the case of Rotaru v. Romania (no. 28341/95) issued on 2 May 2000, the ECHR followed the right to private life taking the form of the right to informational self-determination, while inferring a positive obligation of the State to dispose of the data collected about the individual and relating to their private sphere.

35. A similar approach may also be observed in the judgments of foreign constitutional courts. For instance, the afore-mentioned Federal Constitutional Court of Germany, by means of the right to informational self-determination, guarantees the protection of not only the content of the transferred information but also the external circumstances under which such transfers take place, i.e. the place, time, participants, type and manner of communication, since the knowledge of the communication circumstances may - in association with other data - indicate

the communication content itself, and by means of examining and analysing the data, it is possible to restore the individual profiles of participants to the communication in question. (cf. e.g. the Judgment issued on 27 July 2005, BVerfGE 113, 348 (Vorbeugende Telekommunikationsüberwachung) or the Decision issued on 27 February 2008, BVerfGE 120, 274 (Grundrecht auf Computerschutz).

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

36. In general, the primary objective of the legal regulation concerning the global and preventive collection and retention of traffic and location data on electronic communications is considered to be the protection against security threats and the need to arrange for the accessibility of such data for the purposes of preventing, revealing, investigating and prosecuting serious criminal offences by the public authority. As already pointed out by the Constitutional Court on a number of occasions, prosecuting criminal offences and punishing the offenders rightfully is a constitutionally approvable public interest, whose substance lies in transferring the liability for prosecuting the most serious violations of fundamental rights and freedoms committed by individuals and legal entities onto the State. On condition that the criminal law allows for exercising the public interest to prosecute criminal activity by means of robust tools the use of which results in serious limitations of the personal integrity and fundamental rights and freedoms of an individual, then when applied, constitutional limits have to be respected. Restrictions imposed on personal integrity and individual privacy (i.e. breaching the respect towards them) may only be applied as an absolute exception, provided it is deemed necessary in a democratic society, unless it is possible to meet the purpose pursued by the public interest in any other way and if it is acceptable from the perspective of the legal existence and respecting effective and specific guarantees against arbitrariness. Essential presumptions of a due process require that the individual be provided with sufficient guarantee against the potential abuse of power by the public authorities. Such an essential guarantee consists of the relevant legal regulations and existence of the effective means of monitoring adherence to it, represented by, above all, the supervision of the most intense infringements of the fundamental rights and freedoms of individuals performed by an independent and impartial court, since it is the courts' obligation to provide the protection of individuals' fundamental rights and freedoms (Article 4 of the Constitution of the Czech Republic) [cf. the Judgment file reference I. ÚS 631/05 issued on 7 November 2006 (N 205/43 SbNU 289) and file reference Pl. ÚS 3/09 issued on 8 June 2010 (219/2010 Sb., available in the electronic database of Decisions on http://nalus.usoud.cz)].

37. In its judgments, the conditions outlined above have been specified by the Constitutional Court when assessing the admissibility of the intervention of the public authority to individual privacy taking the form of telecommunication operation interception [cf. e.g. the quoted Judgments file reference II. ÚS 502/2000, file reference IV. ÚS 78/01, file reference I. ÚS 191/05, or file reference I. ÚS 3038/07 issued on 29 February 2008 (N 46/48 SbNU 549)]. The infringement of the individual's fundamental right to privacy in the form of the right to informational self-determination in the sense of Article 10, para. 3 and Article 13 of the Charter, due to the prevention of and protection against criminal activity is thus possible only by means of imperative legal regulations which have to conform

to, above all, the rights arising from the principle of the legal state (rule of law state) and which meet the requirements arising from the proportionality test when, in the case of a conflict between the fundamental rights and freedoms with the public interest or any other fundamental rights and freedoms, the purpose (objective) of such infringement must be assessed in relation to the means applied, whereas it is the proportionality principle (in a broader sense) that provides the standard for such assessment. The wording of such legal regulations must be precise and unambiguous, while also being sufficiently predictable so that it provides potentially affected individuals with sufficient information on the circumstances and conditions under which the public authority is entitled to interfere with their privacy and so that they can act accordingly in order to avoid conflict with the restricting norm. Moreover, the powers granted to the relevant authorities, as well as the manner and the rules of application, must be strictly defined so that individuals are provided with protection against arbitrary infringements. From the perspective of the proportionality principle (in a broader sense), assessing the admissibility of the infringement in question includes three criteria. The first one lies in assessing the eligibility of fulfilling the purpose (or appropriateness as well), where it is determined whether the specific measure itself is capable of achieving the intended purpose, being the protection of another fundamental right or public interest. The second criterion consists in assessing the necessity, i.e. examining whether, upon selecting the appropriate means, the one being most considerate of the fundamental right has been opted for. And finally, it is necessary to assess the adequacy (in a narrower sense), i.e. whether the prejudice to the fundamental right is not disproportionate in relation to the intended purpose, which means that the measures imposing a restriction on fundamental rights and freedoms must not, in case of a collision of the fundamental right or freedom with public interest, exceed (through their negative consequences) the positive aspects represented by the public interest in these measures. [cf. the Judgment file reference Pl. ÚS 3/02 issued on 13 August 2002 (N 105/27 SbNU 177; 405/2002 Sb.)].

38. In case of applying criminal law tools restricting the individual's fundamental rights and freedoms, the essential requirement of court protection of fundamental rights takes the form of the need to issue a court order and its sufficient reasoning. This must conform both to the requirements stipulated by the law, and, in particular, to the constitutional principles on which the legal regulation is based or which limit its interpretation in return, since the application of such regulation represents an exceptional infringement of the fundamental rights and freedoms of every individual. "A court order concerning telecommunication operation interception and retention may only be issued in a properly initiated criminal procedure relating to the criminal activity expressly defined by the law, at the same time being supported by relevant indications based on which a reasoned suspicion that such criminal offence has been committed can be drawn. The order must be individualised in relation to the specific individual using the telephone station. And finally, the court order must, at least to a minimal extent, indicate which facts important to the criminal procedure should be discovered in this way and on what such conclusions are based." (cf. quoted Judgments of the Constitutional Court, file reference II. ÚS 789/06 or file reference I. ÚS 3038/07).

39. A similar approach may also be found in the ECHR judgments. In accordance

with Article 8, para. 2 of the Convention, defining the constitutional limits of the restrictions imposed on fundamental rights and freedoms of individuals, guaranteed by Article 8, para. 1 of the Convention, and when examining every individual case, the ECHR mainly assesses whether the alleged infringement or restriction of the fundamental rights or freedoms may be ranked under the scope of the protection included in Article 8 of the Convention. In the case of an affirmative answer, i.e. provided that the infringement of the right to privacy performed by the public authority took place pursuant to the law which must be accessible and sufficiently predictable, that is expressed with a high level of precision so that it enables the individual to act accordingly if necessary (cf. Malone v. UK, Amman v. Switzerland, or Rotaru v. Romania). The level of precision required in the national legal regulations, which under no circumstances may comprise all possible outcomes, depends, to a large extent, on the content of the examined text, the areas which it is supposed to cover, and the number and status of the persons to whom it is addressed [Hassan and Tchaouch v. Bulgaria (no. 30985/96, 39023/97) issued on 26 October 2000]. In the sense of Article 8, para. 2 of the Convention, the examined infringement of the fundamental rights and freedoms, as guaranteed in Article 8, para. 1 of the Convention, must also be deemed necessary within a democratic society, following the purpose approved by the Convention (e.g. the protection of life or health, national or public security, protection of rights and freedoms of others or morals, preventing unrest or crime, or the interest in economic prosperity of the country), which must be relevant and reasoned in an appropriate manner. For the purposes of examining the accordance of the legal regulation with the Convention, it also has to provide adequate protection against arbitrariness, in the sense of Article 13 of the Convention, and consequently, to define with sufficient clarity the scope and manner of exercise of the powers granted to the relevant public authorities (cf. Kruslin v. France or S. and Marper v. UK). in other words, acts representing an obvious infringement of the fundamental right to private life must not occur beyond any immediate (preventive or subsequent) judicial control [cf. e.g. the Judgment in the case of Camenzind v. Switzerland (no. 21353/93) issued on 16 December 1997].

40. The requirements of the legal regulations allowing the infringement of the right to private life have been specified in more detail by the ECHR in the decisions mentioned above and concerning the assessment of the admissibility of such infringements exercised by the public authority and taking the form of telephone call interception, secret surveillance, or collecting information and data from the individual's private (personal) sphere. The ECHR emphasised that it is, above all, necessary to define clear and detailed rules governing the scope and use of such measures, to determine the minimum requirements concerning the length, mode of retention of the obtained information and data, their use, or the access of third parties, and to establish procedures leading to the integrity and confidentiality of the data, as well as the mode in which the data will be disposed of, so that individuals are provided with sufficient guarantee covering the risk of misuse and arbitrariness. The necessity to be provided with such guarantee grows even higher in the case of the protection of data subject to automatic processing, particularly if the data are due to be used for law enforcement purposes and in the situation when the available technologies are becoming ever more complicated. National law, in particular, must guarantee that the collected data are truly relevant, not being excessive in relation to the purpose for which they were obtained and that

they are retained in the form allowing the identification of the persons for the period not exceeding the necessary extent in order to achieve the purpose for which they were obtained [cf. Preamble and Article 5 of the Convention on the Protection of Data and Principle No. 7 of the Recommendations of the Committee of Ministers No. R(87)15, adopted on 17 September 1987 and concerning the regulation and use of personal data in the police sector, quoted pursuant to the Judgment in the case of Weber and Saravia v. Germany (no. 54934/00) issued on 29 June 2006 or Liberty and others v. UK (no. 58243/00) issued on 1 July 2008].

## VIII. Legal review

### VIII. A) So-called Data Retention

41. As already mentioned by the Constitutional Court, the contested provisions of Section 97, para. 3 and 4 have become part of Act No. 127/2005 Coll., on Electronic Communications, on the basis of Act No. 247/2008 Coll., amending Act No. 127/2005 Coll., on Electronic Communications and on amendments to other related acts (Act on Electronic Communications), as amended. According to the explanatory report, the amendment was adopted for the purposes of implementing "several articles" of the Directive of the European Parliament and Council 2006/24/EC, issued on 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 yet been implemented or have only been implemented in part into our legal system, since the Data Retention Directive has already been transposed into our legal system. [...] In some respects, the legal regulations in force are broader than those contained in the Data Retention Directive." As a matter of fact, the issues of traffic and location data retention have been treated in the Czech legal system, yet in a modified form, upon adopting Act No. 127/2005 Coll., on Electronic Communications, coming into force on 1 May 2005, and upon adopting the contested Decree of the Ministry of Information Technologies No. 485/2005 Coll., on the extent of traffic and location data, time of its storage and the form and method of its disclosure to the bodies authorised to use it, coming into force on 15 December 2005. In the Czech Republic, the Data Retention Directive, under preparation in the EU at that time, was in fact implemented in advance, while the wording of the challenged provisions, already following the requirements laid down by the Data Retention Directive, merely represents a precision of the duty to retain the traffic and location data and to provide it, without any undue delay, to the public bodies authorised to request it. Despite this, the contested Decree of the Ministry of Information Technology has not been amended, which results in the fact that the extent of the retained data, falling under the control of the contested legislation, clearly and obviously remains beyond the extent anticipated by the relevant Data Retention Directive.

42. In accordance with the contested provisions of Section 97, para. 3, sentences one and two of the Electronic Communications Act, the legal entity or natural person operating a public communications network or providing a publicly available electronic communications services is obliged to retain the traffic and location data generated or processed when operating a public communications network or

providing publicly available electronic communications services, including the data on unsuccessful call attempts, on condition that such data are generated or processed and at the same time, retained or recorded. Pursuant to Section 90 of the Electronic Communications Act, the traffic data are deemed as "any data processed for the purposes of transferring or charging for the message through an electronic communications network." Pursuant to Section 91 of the mentioned Act, the location data are defined as "any data processed in the electronic communications network determining the geographical position of the terminal of the user of a publicly available electronic communications service." Pursuant to the contested provisions of Section 97, para. 4, it is the implementing regulations (i.e. the contested Decree No. 485/2005 Coll.) that were entrusted with the specification and the content itself of the traffic and location data, the retention period, and the form and manner of transferring it on to the relevant authorities.

43. Specifically, in the case of fixed network telephone line services and mobile communications services, operators are obliged to collect practically all accessible data on realised phone calls, as well as their unsuccessful call attempts if recorded (referred to as "pings"). The data include, in particular, the information on the type of realised communication, telephone numbers of the person calling and the person called, date and time of commencing and ending the communication, identification of the base station providing the telephone call at the moment of making the connection, identification of the pay-as-you-go telephone card or the public telephone box, and in case of mobile communication, also the data on the unique code identifying every mobile telephony used in the GSM network (IMEI), its position and movement, even if no communication takes place (it is enough when the telephone is switched on), numbers of top-up cards and their association to the relevant telephone number, the connection between a mobile device and all inserted SIM cards, etc. Even higher volumes and extent of data to be retained pursuant to the contested Decree relate to so-called public networks working on the principle of packet switching and the associated services, i.e. most typically the Internet. In the case of using it, the contested legislation provides for the data retention concerning mainly the access to the network (e.g. time, place and length of connection, data on users and their user accounts, identifiers of the computer and the server accessed, IP address, full domain name, volume of transferred data, etc.), as well as the data relating to the access to electronic mailboxes and the transfer of electronic mail messages (in this case, almost all data are retained, except the content of the messages itself, i.e. including address identification, volume of transferred data, etc.), and last but not least, the data on the server and other services [e.g. entered URL address, request type, data on using chat rooms, UseNet, instant messaging (e.g. ICQ), and IP telephony, including the identification of the communicating parties and length and service used (e.g. file transfer or transaction)]. In the case of an Internet connection and email communication, what is monitored and retained beyond the scope of the Data Retention Directive in question is the volume of transferred data, information on applied encryption, method and status of requests to the service and their realisation, as well as information on sending SMS messages from Internet gateways and other "interest identifiers". In the case of telephony and beyond the scope of the Data Retention Directive, the challenged legal regulation requires the retention of data on the identification of the pay-as-you-go card, public telephone box, numbers of top-up cards and their association with the telephone numbers, or the

relations between the mobile devices and inserted SIM cards.

44. Although the prescribed obligation to retain traffic and location data does not apply to the content of individual messages (see Article 1, para. 2 of the Data Retention Directive and the contested provisions of Section 97, para. 3, sentence 4), the data on the users, addresses, precise time, dates, places, and forms of telecommunication 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. As for the statement of the Senate, as summarised above, the opinion of the bill propose that "under no circumstances may this case be compared to interception, since the content of the telephone calls or email messages is not retained" must be regarded as absolutely erroneous, for even on the basis of such data, it is possible to draw sufficient content-related conclusions falling within the scope of the individual's private (personality) sphere. With a degree of certainty of up to 90%, the data allow deducing, for instance whom, how often and even at what times the individual contacts, who their closest acquaintances, friends or work colleagues are, or what activities and at what times they engage in [cf. the study performed by the Massachusetts Institute of Technology (MIT), Relationship Inference, available on http://reality.media.mit.edu/dyads.php]. Collecting and retaining location and traffic data thus also represents a significant infringement of the right to privacy, and for this reason, it is necessary that the scope of the protection of the fundamental right to respect of private life taking the form of the right to informational self-determination (in the sense of Article 10, para. 3 and Article 13 of the Charter) should include not only the protection of the contents of the messages transferred via telephone communication or communication via so-called public networks, but also the traffic and location data related to them.

**VIII. B) Assessing the Contested Legislation from the Perspective of Constitutional Law Requirements**

45. The Constitutional Court was thus invited to assess whether the challenged legal regulation concerning the issues of global and preventive collection and retention of determined traffic and location data on electronic communications (so-called data retention) complies with the constitutional requirements outlined above and allows an infringement of the individual's right to privacy in the form of the right to informational self-determination (in the sense of Article 10, para. 3 and Article 13 of the Charter). Furthermore, with regards to the intensity of such infringement, which in the given case is accentuated by the fact that it affects large and unpredictable numbers of communication participants, since it concerns global and preventive collection and retention of the data in question, the most stringent measures possible have to be applied to meeting the above-mentioned requirements. The Constitutional Court reached the conclusion that the contested legislation does not by far comply with the outlined constitutional law requirements for a number of reasons.

46. The contested provisions of Section 97, para. 3, sentence three of the Electronic Communications Act contain only vague and non-specific determination of duties laid upon legal entities or natural persons retaining the location and traffic data in the above-mentioned scope and extent "to disclose them, upon

request, to the relevant authorities pursuant to a special legal regulation without any undue delay." Although in Section 3, the contested Decree specifies fulfilling the duty towards the competent authorities in individual cases, i.e. it provides a relatively detailed definition of the manner in which the data are handed over, communication mode (electronic), format, programmes used, codes, etc., the wording of the challenged provision of Section 97, para. 3 of the Electronic Communications Act, or even the explanatory report do not specifically imply, in the perspective of the Constitutional Court, the competent authorities or the special legal regulations. With respect to the wording of the provisions of Section 97, para. 1 of the Electronic Communications Act, imposing on legal entities or natural persons operating a public communications network or providing publicly available electronic communications services the duty to provide, at the expense of the complainant, to establish and provide an interface to their network at specific points allowing the connection of an interception terminal, it may only be expected that also in the case of the duty to transmit retained location and traffic data, the law anticipates the same competent authorities and similar special legal regulations addressed to the authorities responsible for criminal proceedings, probably pursuant to Section 88 of the Criminal Procedure Code, the Security Information Service (www.bis.cz) in accordance with Sections 6 - 8a of Act No. 154/1994 Coll., on the Security Information Service, and Military Intelligence in accordance with Sections 9 and 10 of Act No. 289/2005 Coll. and on Military Intelligence. The existing legal regulations allowing for a massive infringement of fundamental rights thus do not comply with the requirements concerning the certainty and clarity from the perspective of the state governed by the rule of law (see Section 37 above).

47. Furthermore, the purpose under which the traffic and location data are provided to the competent authorities has not been defined clearly and precisely, which precludes assessing the challenged legal regulation from the perspective of its actual necessity (whereas it is undoubtedly capable of meeting the purpose, or it is capable of achieving the goal as determined by the Directive - see below). While the Data Retention Directive, referred to above, was adopted in order to harmonise the regulations applied in the Member States and relating to the duties and obligations of publicly available electronic communications services or public communications networks, concerning traffic and location data retention necessary to identify participants or registered users with the aim "to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime" (although it fails to specify the criminal offence in more detail), the contested legislation, let alone the provisions of Section 88a, para. 1 of the Criminal Procedure Code, determining the conditions under which the retained data may be used for the purpose of a criminal procedure, does not contain any such restrictions. In compliance with the legal regulation in question, the possibility to use the retained data in a criminal procedure has not been associated by the legislature with a reasonable suspicion of committing a serious crime. Similarly, the duty of the bodies responsible for criminal proceedings to inform, though subsequently, the affected (monitored) person about this fact has not at all been included in the legal regulation, which mean that it fails to meet the claims arising from the second step of the proportionality test, i.e. the need when selecting the appropriate means, since the above clearly demonstrates that the means the most considerate of the fundamental right to informational self-

determination has not been used.

48. The Constitutional Court does not perceive the manner in which the range of public authorities is (not) defined, as well as the manner (not) defining the purpose for which they are allowed to request the retained data, as sufficient and predictable. Although in compliance with the provisions of Section 88a, para. 1 of the Criminal Procedure Code, as referred to above, the use of retained data is subject to court review, taking the form of a permit issued by the presiding judge (and by the judge within the preliminary procedure), it was the legislature's primary liability to define, with more precision and clarity, both the presumptions and condition of the data use, and the extent of use in the challenged provisions or in the provisions of Section 88a, para. 1 of the Criminal Procedure Code, replacing the absolutely non-specific definition of the conditions determining the use of the retained data "on realised telecommunication operations" for the purposes of "discovering the facts important for the criminal proceedings". With respect to the seriousness and extent of the infringement of the right to privacy in the form of the right to informational self-determination (in the sense of Article 10, para. 3 and Article 13 of the Charter), represented by the use of the retained data, the legislature limited the possibility to use the retained data only for the purposes of criminal proceedings prosecuting serious crime and only in the case that such an objective cannot be achieved using any other means. In fact, this is anticipated not only by the Data Retention Directive, referred to above, but also by the provisions of Section 88, para. 1 of the Criminal Procedure Code, defining the conditions for enacting interception and records of telecommunication operation ("on condition that criminal proceedings related to serious crime have been initiated"), from which the afore-mentioned legal regulation included in the provisions of Section 88a of the Criminal Procedure Code as a whole (despite the legal opinions of the Constitutional Court expressed in the quoted Judgments file reference II. ÚS 502/2000 or file reference IV. ÚS 78/01) deviates without any due reason, providing for the legal regulation in obvious contradiction to the opinions of the Constitutional Court.

49. The absence of proper legal regulation, i.e. in full compliance with the Constitution, as demonstrated by the statistical data has in fact resulted in the situation that the instrument in the form of requesting and using the retained data (including the data on attempted phone calls which are not treated in the Criminal Procedure Code at all), has also been used (or overused) by the bodies responsible for criminal proceedings for the purposes of investigating common (i.e. less serious) crime. For instance, in accordance with the "Report on the Security Situation in the Czech Republic in 2008", the total number of criminal offences recorded in the territory of the Czech Republic amounted to 343,799 (out of which 127,906 offences were detected), while at the same time, the number of requests to provided the traffic and location data made by the competent public authorities reached 131,560 (cf. the corresponding Report of the EU Commission, entitled "The Evaluation of Directive 2006/24/EC and National Measures to Combat Criminal Misuse and Anonymous Use of Electronic Data", having requested the official data from the Czech side, whereas the responses of the Czech Republic in the questionnaire dated on 30 September 2009 are available on http://www.dataretention2010.net/docs.jsp). Unofficial data show that subsequently, in the period from January to October 2009 only, there were 121,839

requests for providing traffic and location data (cf. Herczeg, J.: Constitutional Limits of Telecommunication Operation Monitoring: Conflict between Security and Freedom. Bar Bulletin, Vol. 5/2010, pp. 29).

50. In the view of the Constitutional Court, the legal regulation contested by the applicant fails to define sufficiently, or fails to define at all, unambiguous and detailed rules containing minimum requirements concerning the security of the retained data, in particular, taking the form of restricting third-party access, the procedure of maintaining data integrity and credibility, or the removal procedure. Furthermore, the contested regulation does not provide individuals with sufficient guarantees against the risk of data abuse and arbitrariness. As for the examined case of global and preventive collection and retention of data on electronic communications, the need to have such guarantees available is becoming even more important to the individual owing to the current enormous and fast-moving development and occurrence of new and more complex information technologies, systems and communication tools, which unavoidably results in the borders between private and public space being blurred to the benefit of the public sphere, since in the virtual environment of information technologies and electronic communications (in the so-called cyberspace), every single minute, especially owing to the development of the Internet and mobile communication, thousands or even millions of items of data and information are recorded, collected and virtually made accessible, interfering with the private (personality) sphere of the individual, yet if asked, they would probably be reluctant to knowingly let someone else in.

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

individuals affected, since they do not control the instrument by themselves [see the Judgment file reference Pl. ÚS 15/01 issued on 31 October 2001 (N 164/24 SbNU 201; 424/2001 Coll.) where appropriate]. As a consequence, the actions referred to above, constituting an obvious infringement of the fundamental right to privacy in the form of the right to informational self-determination (in the sense of Article 10, para. 3 and Article 13 of the Charter) and due to the legal regulation being considered as insufficient and failing to meet the afore-mentioned constitutional requirements, occur beyond the scope or reach of any immediate (yet subsequent) review, particularly a judicial one, the necessity of which has also been expressed by the ECHR in the Decision concerning the case of Camenzind v. Switzerland, referred to above.

52. Similar conclusions have also been drawn by Constitutional Courts in other European countries when examining the constitutionality of legal regulations implementing the afore-mentioned Data Retention Directive. For instance, in its Decision issued on 2 March 2010 (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), the Federal Constitutional Court of Germany, held that the contested legislation concerning the issues of preventive data retention (Vorratsdatenspeicherung) (in the sense of Sections 113a and 113b of Telekommunikationsgesetz) and their use within criminal proceedings (in the sense of Section 100g, para. 1 of Strafprozessordnung) was unconstitutional due to a contradiction with Article 10, para 1. of the Constitution protecting the inviolability of correspondence, mail and telecommunications. The Federal Constitutional Court of Germany held that the challenged legal regulation failed to comply with the requirements arising from the proportionality principle, requiring - among other things - that the legal regulation concerning data retention should correspond to the seriousness of the infringement of individuals' fundamental rights. Specifically, the contested legislation failed to provide a sufficient definition regarding the purpose of the use of the data, failed to guarantee their sufficient security, and last but not least failed to provide the individual with sufficient, adequate and effective guarantees against the risk of misuse, mainly in the form of judicial review. The federal legislation was invited to comply with these requirements pursuant to Article 73, para. 1, clause 7 of the Constitution. Similar conclusions were also adopted by the Constitutional Court of Romania in its Decision issued on 8 October 2009 (No. 1258), declaring the relevant legal regulation as unconstitutional, since it failed to define the purpose of use of such an instrument, its wording remained too vague without specifying, in more detail, the powers and obligations of the competent public authorities, and failed to provide the individuals affected with sufficient protection against misuse due to the absence of judicial review (the unofficial English translation of the Decision is available on http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanianconstitutional-court-decision-regarding-data-retention.html). Similar approaches were also taken by the Supreme Court of Bulgaria in its Decision issued on 11 December 2008 (information available on http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention) and the Supreme Court of Cyprus in its Decision issued on 1 February 2011 (information available on http://www.edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus).
According to the information of the Constitutional Court, the legal regulations implementing the afore-mentioned Data Retention Directive are currently being examined in Poland and Hungary. The necessity to provide, in a manner as stringent as possible, the guarantees and instruments for protecting the

fundamental rights of individual when handling their personal data generated in course of electronic communications was also emphasised by the European Court of Justice in its preliminary ruling issued on 9 November 2010 concerning the joint case of Volker und Markus Schecke GbR GbR and Hartmut Eifert v. Land Hessen (C-92/09 a C-93/09).

53. With respect to the above, the Constitutional Court holds that the challenged provisions of Section 97, para. 3 and 4 of Act No. 127/2005 Coll., on Electronic Communications and on Amendments to Certain Related Acts (Electronic Communications Act), as amended, and the contested Decree No. 485/2005 Coll., on the extent of traffic and location data, time of its storage and the form and method of its disclosure to the bodies authorised to use it, cannot be deemed as constitutionally conforming, since they are in obvious contradiction to the afore-mentioned constitutional limits, for they fail to meet the requirements arising from the rule of law state principles and are in collision with the requirements concerning the restrictions imposed on the fundamental right to privacy in the form of the right to information self-determination in the sense of Article 10, para. 3 and Article 13 of the Charter, based on the proportionality principle.

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.

**VIII. C) Obiter dictum**

55. Taking the form of an obiter dictum only, the Constitutional Court maintains that it is aware of the fact that owing to the development of modern information technologies and communication means, new and more sophisticated ways of commitment of crime occur, which need to be addressed accordingly. Nonetheless, the Constitutional Court expresses its doubts whether the very instrument of global and preventive retention of location and traffic data on almost all electronic communications may be deemed necessary and adequate from the perspective of the intensity of the intervention to the private sphere of an indefinite number of participants to electronic communications. Within the European context, such opinion is not at all rare, since the Data Retention Directive has faced substantial criticism since its coming into force, both from the Member States (e.g. the governments of Ireland, the Netherlands, Austria or Sweden have been hesitating to implement it or have not implemented it yet, whereas the latter two have done so despite a publicly announced warning of the Commission to initiate proceedings with the European Court of Justice), and from legislators in the European

Parliament, the European Data Protection Supervisor (see the data retention conference conclusions held by the Commission in Brussels on 3 December 2010, available on http://www.dataretention2010.net/docs.jsp), or the Data Protection Working Group established in accordance with Article 29 of Directive 95/46/EC (cf. its statements available on http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm ), as well as from non-governmental organisations (such as Statewatch, European Digital Rights or Arbeitskreis Vorratsdatenspeicherung - AK Vorrat). All the bodies mentioned above have sought to put the location and traffic data with more adequate instruments (e.g. so-called data freezing allowing the monitoring and retention of necessary and certain data relating to the specific participant to communication selected in advance, provided certain conditions are met), or they have sought its amendments, mainly in the form of providing the individuals affected with sufficient guarantees and means of protection, as well as applying more restrictions on retained data security against threats of third-party leaks and misuse.

56. Similarly, the Constitutional Court expressed its doubts when also examining whether the instrument of global and preventive retention of traffic and location data may be deemed, from the perspective of the original purpose (i.e. protection against security threats and prevention of serious crime) as an effective tool, mainly due to the existence of so-called anonymous SIM cards, which are beyond the extent of retained location and traffic data as anticipated within the contested legislation and which, according to reports of the Police of the Czech Republic, are used for the purposes of commitment of criminal offences up to a level of 70% (cf. "Czech Police in bid to ban anonymous SIMs, operators protest", iDNES.cz, 18 March 2010). In this respect, it is possible to refer to the analysis of the Federal Investigation Bureau of Germany, dated 26 January 2011, which - on the basis of comparing data before and after adopting the legal regulation in question - concluded that using the instrument of global and preventive retention of location and traffic data produced only negligible effect in reducing the number of serious crimes or the level of their detection (the analysis and the specific statistic data are available on http://www.vorratsdatenspeicherung.de/content/view/426/79/lang,de/). Similar conclusions may also be drawn when glancing at the statistic summaries of crimes committed in the territory of the Czech Republic, e.g. the comparison of statistic data in the period of 2008 – 2010 (available on http://www.policie.cz/clanek/statisticke-prehledy-kriminality-650295.aspx).

57. Last but not least, the Constitutional Court would like to express its doubts whether it is at all desirable that private persons (service providers in the area of the Internet, telephone and mobile communication, i.e. in particular, mobile operators and commercial enterprises providing Internet access) should be entitled to retain all data on the communication provided by them, as well as on customers to whom services are provided (i.e. data going beyond the extent of data which they are obliged to retain in accordance with the contested legislation), or that they should be allowed to dispose of them freely for the purposes of collecting debts or developing their business or marketing activities. The Constitutional Court perceives such a situation as undesirable mainly due to the fact that the Electronic Communications Act or any other legal regulations do not specify or define this

competence and its purpose in further detail; the rights and duties have not been defined in a sufficient and precise manner, as well as the extent of retained data, the length and manner of retention, and the requirements concerning the data security or review mechanisms have not been specified in further detail, either.

58. With respect to the above, the Constitutional Court held, in accordance with Section 70 para. 1 of the Constitutional Court Act that the contested provisions of Section 97, para. 3 and 4 of Act No. 127/2005 Coll., on Electronic Communications and on Amendments to Certain Related Acts (Electronic Communications Act), as amended, and the contested Decree No. 485/2005 Coll., on the extent of traffic and location data, time of its storage and the form and method of its disclosure to the bodies authorised to use it, should be abolished on the day of publishing the Judgment hereof in the Collection of Laws (Section 58, para 1. of the Constitutional Court Act).

59. General courts will have to engage in examining, in each and every individual case, the application of the already requested data for the purposes of criminal proceedings from the perspective of the proportionality of the infringement of the right to privacy. Above all, courts will have to consider the seriousness of the crime committed upon the act against which criminal proceedings have been initiated and in which the requested data should be used.

Notice: No Appeal against Decisions of the Constitutional Court is permissible. (Section 54, para. 2 of the Constitutional Court Act)

Brno, 22 March 2011

Pavel Rychetský
Chief Justice of the Constitutional Court