Czech Republic
FINDING
of the Constitutional Court

In the Name of the Republic

The Constitutional Court, sitting in full court, composed of 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), decided, on 22 March 2011, on an application from a **group of deputies of the Chamber of Deputies of the Parliament of the Czech Republic,** represented by the deputy Marek Benda, Praha 1, Sněmovní 4, for the annulment of Section 97(3) and (4) of Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended, and for the annulment of Decree No 485/2005 on the scope of traffic and location data, the period of retention thereof, and the form and method of transmission thereof to bodies authorised to use them, with the participation of the Chamber of Deputies and the Senate of the Parliament of the Czech Republic as parties,

as follows:

Section 97(3) and (4) of Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended, and Decree No 485/2005 on the scope of traffic and location data, the period of retention thereof, and the form and method of transmission thereof to bodies authorised to use them are annulled as of the date of publication of this Finding in the Collection of Laws.

Grounds:

I.
Summary of application

1. A group of 51 deputies of the Chamber of Deputies of the Parliament of the Czech Republic, in an application filed with the Constitutional Court on 26 March 2010, sought the annulment of Section 97(3) and (4) of Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended (hereinafter also referred to as "contested provisions"), and Decree No 485/2005 on the scope of traffic and location data, the period of retention thereof, and the form and method of transmission thereof to bodies authorised to use them (hereinafter also referred to as the "contested Decree" or collectively also as the "contested legislation").

2. Although the application met the formal requirements under Article 87(1)(a) of the Constitution of the Czech Republic and Section 64(1)(b) of Act No 182/1993 on the Constitutional Court, as amended (the "Constitutional Court Act"), the Constitutional Court considers it necessary to emphasise that the concept of an application for the annulment of an act or its individual provisions under Article 87(1)(a) of the Constitution of the Czech Republic, filed by a group of deputies or senators pursuant to Section 64(1)(b) of the Constitutional Court Act, is also a manifestation of the constitutionally guaranteed principle of the protection of minorities (Article 6 of the Constitution of the Czech Republic) and primarily serves as one of the tools for the protection of the parliamentary minority (the

opposition) against possible arbitrariness in decisions taken by a parliamentary majority in the legislative process, based on the principle of majority decision-making [cf. the report of the Venice Commission CDL-AD(2010)025 "*Report on the Role of the Opposition in a Democratic Parliament*" of 15 November 2010, which includes the right of the parliamentary opposition to the constitutional review of decisions (laws) adopted by the majority among the most fundamental rights of the parliamentary opposition]. In other words, a qualified submission to the impartial and independent Constitutional Court is often the last resort for a parliamentary minority seeking to defend itself against arbitrariness in the decision-making of the parliamentary majority because, by number, representatives of the parliamentary opposition are usually in a numerical minority in Parliament and so do not have effective means to reverse or change the adoption of such a decision (the issuance of a legislative act) in the legislative process. On the contrary, representatives of the parliamentary majority generally do have such effective means, and where they have doubts about the correctness, soundness, or even the constitutionality of the decisions they are adopting (or have previously adopted), it is not only their right, but also their duty, to use them for this purpose (see the oath pursuant to Article 23(3) of the Constitution of the Czech Republic). The concept of filing an application with the to the Constitutional Court for the annulment of an act or individual provisions thereof under Article 87(1)(a) of the Constitution of the Czech Republic in no way serves as a means to obtain an expert opinion of the Constitutional Court on a decision adopted by the parliamentary majority, nor as an instrument used as a manifestation of a political or even pre-election struggle transferred from Parliament to the Constitutional Court. In the present case, not only is the group of applicants composed mainly of representatives of political parties which currently contribute to and, at the time of the application, contributed to the exercise of governmental power, and held, and continue to hold, a majority in the Parliament of the Czech Republic needed to change the contested legislation, but the Constitutional Court is also compelled to note, with criticism, that the overwhelming majority of this group, by voting in favour (!) during the legislative process, contributed directly to the adoption of the contested legislation. In such cases of (mis)use, the Constitutional Court would be forced to dismiss such applications in the future.

3. The essence of the objections was summed up by the applicants themselves to the effect that the collection and use of traffic and location data on telecommunications traffic to the extent defined by the contested provisions and the contested Decree constitutes disproportionate interference with fundamental rights set out in the Charter of Fundamental Rights and Freedoms (hereinafter referred to as the "Charter") and the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter referred to as the "Convention"), specifically the fundamental rights guaranteed by Article 7(1), Article 10(2) and (3), and Article 13 of the Charter and Article 8 of the Convention. According to the applicants, this interference may also be regarded as undermining the essential requirements of the democratic rule of law, including the principle of proportionality within the meaning of Article 4(4) of the Charter. The applicants relied on the following arguments to support their allegations.

I. A) The collection of data on communications as an interference in private life

4. The content of the contested provisions is the obligation for natural and legal persons providing a public communications network or publicly available electronic communications service (i.e. primarily telephone operators and Internet service providers), to retain, for a period of six to twelve months, traffic and location data (dozens of fields of data) on all telephone and fax communications, e-mail and SMS communications, website visits and use

of certain Internet services, as specified in the contested Decree, which they are required to disclose to authorised institutions on request. According to the applicants, the above data, the collection and storage thereof, and the transmission thereof to government authorities clearly fall under the protection of Article 8 of the Convention. In this context, they referred to numerous decisions by the European Court of Human Rights (hereinafter referred to as the "ECHR") and the Constitutional Court.

5. The applicants also believe that interference with fundamental rights encompasses not only a direct breach (e.g. familiarisation with the data retained), but also measures by government authorities concealing a significant risk of restrictions on fundamental rights, which could occur at any moment. The retention of traffic and location data cannot but be regarded as such an interference because they are continuously stored, are available to government authorities, and can be requested and used in the future under relevant rules. Therefore, the retention of the above data carries a latent risk of further direct interference by government authorities. Moreover, the fact that the State does not retain traffic and location data itself, but uses private persons providing telecommunications services for this purpose, cannot be overlooked; the risk of the potential abuse of such retained data by a large number of private persons working in the field of telecommunications services is higher than if the data were retained by the State. One of the ECHR's basic requirements, developed by an interpretation of the condition of the legal basis for government interference with private life, is the predictability and availability of such a legal basis. The reason for this is the legitimate and logical requirement for individuals to be acquainted in advance with the circumstances in which the State may, exceptionally, interfere with their private lives, so that they can adjust their behaviour in order to avoid such interference. The blanket nature of the retention of traffic and location data, however, limits, and even excludes, such a possibility.

6. According to the applicants, the objectives, as well as the probable and expected benefit arising from the obligation to retain traffic and location data, are grossly disproportionate to the associated interference with the fundamental rights of the individuals concerned. Therefore, in accordance with Article 8(2) of the Convention, they assessed the adequacy of this measure in terms of the seriousness and extent of interference with the fundamental rights of individuals (in this case their right to privacy), the legitimacy of the objective to be attained by the restriction of fundamental rights to serve, and the benefit of such interference. Finally, they juxtaposed its use with the associated dangerous aspects, especially the risk of misuse of the data retained.

I. B) The seriousness and extent of interference with the right to privacy

7. First, the applicants noted that the introduction of the obligation to retain traffic and location data constitutes a serious invasion of privacy, because these data open up broad possibilities for their use; combining them with other data could have very serious repercussions on the private lives of the individuals concerned. The obligation to retain traffic and location data to such an extent virtually excludes the existence of uncontrolled and unmonitored telecommunications, which must be regarded as particularly intense interference with the privacy of all persons using telecommunication devices (telephony, Internet services), which are no longer used for interpersonal communication, but also encompass a wide range of everyday activities (shopping, banking, education, medicine, etc.). Numerous other (in many cases very sensitive) data and information about a person and his privacy can be inferred from the data retained. In many cases, sensitive information about the sender (e.g. if the addressee is a medical specialist) can be revealed by the identity of the recipient of a

call or e-mail; similarly, information on the opinions, health status or sexual orientation of a person can be ascertained from his online browsing history. Large amounts of information can also be obtained from location data on the movement of a mobile telephone (or holder thereof), especially in combination with location data on the movement of other mobile phones (an indication of who has met whom where and when, etc.). The data retained can be used to build up a communication and movement profile of an individual, not only providing information about past activities, but also predicting, with a high of probability and accuracy, his future activities, which also constitutes significant interference with an individual's right to the protection of privacy and correspondence.

I. C) The legitimacy of the objective and benefit of interference with fundamental rights

8. In their application, the applicants also disputed the legitimacy of the aim of adopting the contested legislation. The Government's explanatory memorandum discussing Section 97 of the Electronic Communications Act indicates that the purpose of Section 97 is to counter increasing security risks and ensure the security and defence of the Czech Republic, but fails to explain this in more detail. The applicants are of the opinion that, under Article 8(2) of the Convention, an invasion of privacy is permissible in fighting crime only if it serves to prevent crime. "The preventive, general retention of telecommunications data for no concrete reason tends to home in on the past, and as such can serve mainly to solve crimes which have already been committed." (p. 13). In the applicants' opinion, interference with privacy in order to solve a crime that has already been committed contravenes Article 8 of the Convention. Furthermore, the data is retained in the absence of any particular suspicion. The contested provisions view all persons as suspects even where there are no specific circumstances to justify such suspicions, which is inadmissible in the rule of law. The applicants also pointed out (with reference to specific cases from abroad) that assessments of data on telecommunications traffic raise the risk of misinterpretation and the suspicion or accusation of innocent people. The person who actually engaged in communication may even be confused with the person who, for example, signed the contract with the telephone operator or Internet service provider.

9. The applicants claim that neither the submitter of legislation nor the competent government authority provided information as to the number or specific cases, before the introduction of the contested legislation (which entails a huge increase in the quantity of and potential access to the data retained), in which the investigation, detection and prosecution of serious crimes collapsed due to the inability to obtain the required data because such data were not available. Nor is it known whether the establishment of the obligation to retain all data on telephone and electronic communications, compared with previous legislation, will genuinely result (or has genuinely resulted) in the improved investigation, detection and prosecution of serious crimes, the aversion of threats, a higher crime-solving rate or a reduction in crime, etc. Furthermore, it is not known how far back authorised bodies may go in their requests for data, and, therefore, to what extent it is necessary to retain traffic and location data for six months or longer. Moreover, interference in private life, paradoxically, may often relate to persons who are not involved in serious crime rather than those who commit it and, as such, are quicker to engage in anonymous communication. According to the applicants, data retention can help to meet stated objectives only on a minor scale and in less important cases; in this respect, a long-lasting, positive impact on crime reduction and increased security in connection with telecommunications use cannot be expected.

I. D) Risk of misuse of retained data

10. Likewise, according to the applicants, there is a risk that the data retained will be used illegally or misused, since, considering the large number of companies that provide telecommunications (especially mobile communications and the Internet), the corresponding security of such traffic and location data is unrealistic. It is therefore necessary to examine realistic and technically existing possibilities for the use of such data. In the view of the applicants, the contested legislation fails to lay down the conditions under which data are to be retained and the conditions for their use by authorised bodies; nor do they make any guarantee to individuals that the data will not be misused. The contested legislation thus encourages the extensive use of the relevant databases, both in terms of the quantity of data drawn from them and as regards the number of entities that will be authorised to access them; it also allows for an expansion in the purposes for which the data will be used. The applicants believe that there is a very real risk of third-party misuse of traffic and location data. The persons who could misuse the personal data are often the employees of companies or government authorities processing the data, as well as others (e.g. hackers).

I. E) Question referred to the European Court of Justice for a preliminary ruling

11. At the end of their application, the applicants express the belief that, while the contested legislation is national legislation subject to criteria arising from the Czech Republic's constitutional architecture, it is also a subject whose origins stem from Community law, namely the transposition of Directive 2006/24/EC of the European Parliament and of the Council EC (hereinafter referred to as the "Directive on Data Retention") into Czech law. In this light, for the same reasons discussed above, the applicants presented the Constitutional Court, for its consideration, with the possibility of submitting a question to the European Court of Justice for a preliminary ruling in accordance with Article 234 of the EC Treaty, concerning the (in)validity of the Data Retention Directive itself, since there is a significant risk that the Directive in question, which was transposed into Czech law by means of the contested provisions and the contested Decree, is in conflict with EC law.

II.
Summary of the parties' observations

12. The Constitutional Court, in accordance with Section 42(4) and Section 69 of the Constitutional Court Act, sent the application for the annulment of the contested provisions and the contested Decree to the Chamber of Deputies and the Senate of the Parliament of the Czech Republic, as well as to the Ombudsman.

13. In a statement of 26 April 2010, the Chamber of Deputies of the Czech Republic, represented by its Chairman, Mr M Vlček, described in detail the procedure for adopting the government bill amending Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended, under which the contested provisions became part of Act No 127/2005 on electronic communications (see Part IV of the Finding). Moreover, the content of the government bill noted that, in the explanatory memorandum, the Government had expressly stated that the submitted bill was consistent with the constitutional and legal order of the Czech Republic and did not contradict international treaties by which the Czech Republic is bound. The Chamber of Deputies based

their debate on the same premise. It is therefore up to the Constitutional Court to examine the constitutionality of the contested provisions.

14. In its statement of 28 April 2010, the Senate of the Parliament of the Czech Republic, represented by its Chairman, Mr P Sobotka, after extensively summarising the applicants' arguments contained in the application under consideration, also described the procedure followed by the Senate in adopting the government bill (see Part IV of the Finding). Regarding the course of its discussions, it also pointed out that the bill was presented to the Committee on the Economy, Agriculture and Transport, the Standing Senate Commission on the Media, and, later, the full Senate as another amendment responding to the Czech Republic's obligation to transpose the relevant EC Directive into national law. As to the obligation of telecommunication operators, Internet service providers and others working in the field of electronic communications to store location and traffic data for at least six months, the submitter pointed out that "*in no way can this be likened to tapping, if only because the content of individual calls or email messages is not stored, and because it concerns Internet services (...), location and traffic data, i.e. technical data, are retained*". The Senate accepted this when debating the draft amendment in question and, following the advice of the Committee and the Standing Senate Commission on the Media, approved the bill in the wording adopted by the Chamber of Deputies. It is therefore now left to the Constitutional Court to examine the application for the annulment of the provisions of the Electronic Communications Act in question and to reach a final decision.

15. In his statement of 12 April 2010, the Ombudsman, Mr Otakar Motejl, declared, after studying the application that had been sent to him, that he disagreed with the arguments put forward, and therefore he would not intercede in proceedings to annul the contested Decree before the Constitutional Court.

III.
Waiving the hearing

16. According to Section 44(2) of the Constitutional Court Act, the Constitutional Court may, with the consent of the parties, waive the hearing process if no further clarification of the case can be expected from a hearing. Therefore, the Constitutional Court, in accordance with the above provision, asked the parties whether they were willing to forego a hearing. The applicants and the Senate of the Parliament of the Czech Republic expressed agreement; the Chamber of Deputies of the Parliament of the Czech Republic did not respond by the designated deadline. In this light, the hearing process in the case under consideration could be waived.

IV.
Constitutional conformity of the procedure for adopting the contested provisions of the Act and statutory conditions for the adoption of the contested Decree

17. In the procedure for examining standards pursuant to Article 87(1)(a) of the Constitution of the Czech Republic, the Constitutional Court Act, within the meaning of Section 68(2), must first consider whether the law in question was adopted and promulgated in the constitutionally prescribed manner (for more on the algorithm of reviews in the procedure for examining standards, see paragraph 61 of Finding Pl. ÚS 77/06 of 15 February 2007 (N 30/44

SbNU 349; 37/2007 Sb.)]. In the case of subordinate legislation, specifically the decrees of ministries, the Constitutional Court, pursuant to Section 68(2) of the Constitutional Court Act, assesses whether it was passed and promulgated within the bounds of the authority prescribed by the Constitution of the Czech Republic (Article 79(3) of the Constitution of the Czech Republic), i.e. whether it was issued "ultra vires".

18. The Constitutional Court made the following findings based on statements from both chambers of the Parliament of the Czech Republic, the attached appendices and documents available electronically (resolutions and printed documents available in the digital library on the websites of the Chamber of Deputies and the Senate at www.psp.cz and www.senat.cz): The contested provisions of Section 97(3) and (4) became part of Act No 127/2005 on electronic communications on the basis of Act No 247/2008 amending Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended. The bill was submitted to the Chamber of Deputies by the Czech Government on 16 January 2008; the Government proposed that the bill be debated in such a manner that the Chamber of Deputies could pass it in the first reading. The bill was distributed to deputies on 18 January 2008 as Parliamentary Press No 398/0 *Amendment to the Electronic Communications Act – EU*. In the first reading, which took place at the 27th session on 30 January 2008, the Chamber of Deputies refused to debate the bill in such a manner that it could be passed in the first reading. The bill was then assigned to the Economic Committee, the Constitutional Law Committee and the Committee on Security (Resolution No 593) for consultation. These committees discussed the bill; their resolutions, containing amendments, were delivered to deputies as Press Nos 398/1, 398/2 and 398/3. Only the amendments put forward by the Committee on Security concerned the contested provisions of Section 97(3) (the third and fifth sentences). At the 28th session of the Chamber of Deputies, the second reading was held on 20 March 2008 and 25 March 2008. The bill underwent general and detailed debate, during which amendments were also proposed to the contested provisions (Section 97(3), third and fifth sentences, and Section 97(4)) by individual deputies (amendments were proposed by Ms Z Bebarová-Rujbrová , Ms K Jacques and Mr J Klas). The proposed amendments were prepared as Press No 398/4, which was distributed to deputies on 25 March 2008. The third reading took place on 23 April 2008 at the 30th session of the Chamber of Deputies. The proposed amendments to the contested provisions of Section 9793) and (4) were not adopted. The bill was approved in the wording of further amendments (Resolution No 736) after the Chamber of Deputies expressed its approval; of the 176 deputies present, 89 voted for and 21 against the bill, with 66 abstentions (Vote No 44).

19. The Chamber of Deputies referred the bill to the Senate on 19 May 2008. The Senate's Organisation Committee designated it for discussion by the Committee on the Economy, Agriculture and Transport as Senate Press No 247. In addition, the bill was also discussed by the Standing Senate Commission on the Media. At its meeting held on 28 May 2008, the committee adopted Resolution No 270, in which it recommended that the Senate approve the bill. The Standing Senate Commission on the Media also recommended that the Senate approve the bill (Resolution No 22 of 4 June 2008). The Senate debated the bill on 5 June 2008 at its 14th session (sixth term) and adopted Resolution No 402 on the bill, approving the bill in the wording in which it was referred to the Senate by the Chamber of Deputies. Of the 52 senators present, 38 voted in favour of the resolution and two were against, with 12 abstentions (Vote No 29).

20. The Act was delivered to the President for signature on 11 June 2008 and was signed by him on 25 June 2008. The approved Act was then delivered to the Prime Minister for his

signature on 30 June 2008. *The Act was promulgated on 4 July 2008 in the Collection of Laws, Volume 78, under number 247/2008, with effect as of 1 September 2008.*

21. The contested Decree No 485/2005 on the scope of traffic and location data, the period of retention thereof, and the form and method of transmission thereof to bodies authorised to use them was issued by the Ministry of Informatics of the Czech Republic. The authority of ministries to issue implementing legislation is based on Article 79(3) of the Constitution of the Czech Republic. Materially, however, this is contingent on the existence of express statutory authorisation and the limits thereof. In the present case, this authorisation is the contested provisions of Section 97(4) of Act No 127/2005 on electronic communications. The Decree was signed by the Minister for Informatics and duly published in Volume 169 of the Collection of Laws under number 485/2005, with effect as of the date of publication, i.e. 15 December 2005.

22. The Constitutional Court notes that both Act No 247/2008, by which the contested provisions were inserted into Act No 127/2005 on electronic communications, and the contested Decree No 485/2005 were adopted in a manner anticipated by the Constitution.

V.
Text of the contested provisions of the Act and the contested Decree

23. The contested provisions of Section 97(3) and (4) of Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended, read as follows:

Section 97

(3) A legal or natural person providing a public communications network or providing a publicly available electronic communications service shall retain traffic and location data which are generated or processed in the provision of its public communications networks and in the provision of its publicly available electronic communications services.[37b)] *A legal or natural person providing a public communications network or providing a publicly available electronic communications service shall retain traffic and location data relating to unsuccessful call attempts only if these data are generated or processed and retained or recorded at the same time. A legal or natural person who retains traffic and location data in accordance with sentences one and two shall, upon request, immediately provide them to authorities authorised to request them pursuant to special legislation. At the same time, this person shall ensure that the content of reports is not retained with the data referred to in sentences one and two. The period for the retention of traffic and location data shall not be less than six months or more than 12 months. After this period, a person who retains data pursuant to sentences one and two shall destroy them, unless such data have been provided to authorities authorised to request them under special legislation or unless otherwise provided by the present Act (Section 90).*

(4) The scope of traffic and location data retained in accordance with paragraph (3), the period for the retention thereof in accordance with paragraph (3) and the form and method of their transmission to authorities authorised to use them, and the period for the retention and disposal of data provided to authorities authorised to request them under special legislation, shall be laid down in implementing legislation.

[37b)] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.*

24. The contested Decree No 485/2005 on the scope of traffic and location data, the period of retention thereof, and the form and method of transmission thereof to bodies authorised to use them reads as follows:

485/2005
DECREE
of 7 December 2005

on the scope of traffic and location data, the period of retention thereof, and the form and method of transmission thereof to bodies authorised to use them

The Ministry of Informatics, in cooperation with the Ministry of the Interior, provides for the following, pursuant to Section 150(3) of Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended by Act No 290/2005 and Act No 361/2005 (hereinafter referred to as the "Act"), in order to implement Section 97(3) of the Act:

Section 1

For the purposes of this Decree
a) "BTS station" shall mean the base station of a public mobile telephone network;
b) "StartBTS station" shall mean the base station of a public mobile telephone network to which the subscriber is allocated at the start of communication;
c) "StopBTS station" shall mean the base station of a public mobile telephone network to which the subscriber is allocated at the end of communication;
d) "IMEI number" shall mean international mobile equipment identity;
e) "MSISDN number" shall mean a subscriber number in a public mobile telephone network;
f) "IMSI number" shall mean the international identifier of a public mobile telephone network subscriber;
g) "destination" shall mean the designation of a foreign operator's network;
h) "URI identifier" shall mean a uniform resource identifier;
i) "code of a legal or natural person providing a public communications network or providing a publicly available electronic communications service" shall mean the serial number of a certificate in the register of entrepreneurs pursuant to Section 14 of the Act.

Section 2
Scope of retention of traffic and location data

(1) A legal entity or natural person providing a publicly available communications network or electronic communications service (hereinafter referred to as an "operator") shall provide traffic and location data defined by this Decree (hereinafter referred to as "data") to an authority authorised to request such data (hereinafter referred to as "authorised authority").

(2) With regard to electronic communications networks with circuit switching and a fixed connection, the following shall be retained:
a) data on communications made, indicating the type of communication, the subscriber's calling and called telephone numbers, or the identifier of a telephone card for use in public pay telephones, the date and time of the initiation of communication, the length of communication, and where appropriate the communication status,
b) data on all public pay telephones with their telephone number, registration number, geographic coordinates and a verbal description of the location.

(3) With regard to public mobile telephone electronic communications networks, the following shall be retained:
a) data on communications made, with an indication of the type of communication, the subscriber's calling and called telephone number, the date and time of the initiation of communication, the length of communication, the IMEI number, the StartBTS station number, and where appropriate the StopBTS station number, destination and additional information,
b) data on the links between MSISDN numbers and IMEI numbers used together in a network, the identification of the BTS and the IMEI number mediating calls without a SIM card to the emergency number "112", the IP addresses of terminals used to mediate the sending of text messages via the Internet , the date and time of the topping-up of credit in relation to prepaid services, the numbers of top-up coupons for a subscriber's given telephone number, the subscriber's telephone number in relation to a given top-up coupon,
c) data on all BTS stations, with an indication of their number, geographic coordinates, antenna direction azimuth and verbal description of the location of the BTS station.

(4) With regard to electronic communications networks with packet switching, data on communications made shall be retained
a) in respect of the services of access to the network indicating the type of connection, the service user equipment ID, the date and time of the opening of the connection, the date and time of the closing of the connection, interest identifiers (e.g. the IP address, port number), the event status (e.g. success, failure, ordinary or extraordinary closure of the connection), the quantity of data transmitted (incoming/outgoing),
b) in respect of services of access to e-mail accounts with an indication of the identifier of the interest user equipment, user account, identifier of a message in the e-mail server, the date and time of the initiation of communication, the e-mail address of the sender, the e-mail address of the recipients, the e-mail protocol identifier, the quantity of data transmitted, information on the use of secure communication,
b) in respect of services of e-mail message transmission with an indication of the identifier of the interest user equipment, identifier of the e-mail server, the date and time of the initiation of communication, the e-mail address of the sender, the e-mail address of the recipients, the e-mail protocol identifier, the quantity of data transmitted, information on the use of secure communication,
d) in respect of server services with an indication of the identifier of the interest user equipment, user account identifier, the date and time of the service request, all server identifiers (in particular the IP address, the complete domain name FQDN), the requested identifiers of the URI or type of service, additional parameters of the URI or service identifiers, the services used, the quantity of data transmitted, the method and status of a service request,
e) in respect of other electronic communications services (in particular for chat, usenet, instant messaging and IP telephony services), with an indication of all the identifiers of the communicating parties, the transport protocol, the date and time of the initiation of communication, the date and time of completion of the communication, the services used, the quantity of data transmitted.

Section 3
Method for the transmission of data

(1) An authorised authority shall request the provision of retained data from the operator through its designated liaison office. The operator shall transmit the requested information without undue delay through its designated liaison office. The data pursuant to Section 2(3)(c) shall be transmitted collectively on a regular basis once a month in their current state as at the date of transmission.

(2) Communication between the liaison offices of the operator and authorised authority shall take place preferably in a manner allowing remote access. Requests and data shall be transmitted preferably in electronic form as data files. In the communications of liaison offices, only generally available technology and communication protocols shall be used so that the solution is not tied to a particular manufacturer or supplier.

(3) Where a method facilitating remote access cannot be used for communications or if the use of such a method would be inexpedient, a request or requested data may be transmitted in paper form or in the form of data files on a portable medium.

(4) The following shall be used to demonstrate the authenticity of a request or requested data:
a) an advanced electronic signature based on a qualified certificate issued by an accredited provider of certification services;[1)] the format of a cryptographic standard with the public key PKCS # 7 shall be used for the creation and authentication of the signature,
b) a cover letter in paper form containing the reference number or serial number of the request, the file name, date, time and method of transmission and, where appropriate, the checksum or standard hash file (e.g. SHA-1) and the signature of the authorised person,
c) a letter in paper form containing the reference number and signature of the authorised person, or
d) in the case of requests or data already submitted in electronic form over a certain period (usually one week), in respect of which no other method was used to prove the authenticity thereof, a letter in paper containing the reference number and signature of the authorised person, which shall sent subsequently.

(5) Data on communications made under an identifier over a specific time period shall be transmitted by the operator to the authorised authority as a) a listing of communications from a fixed line, in respect of data under Section 2(2)(a); b) a listing of mobile communications, in respect of data under Section 2(3)(a); c) a listing of data communications, in respect of data under Section 2(4).
(6) The listings pursuant to paragraph (5) shall be transmitted to the authorised authority in a structured text file, preferably encoded according to the character set CP-1250, UTF-8 or ISO 8859-2. The files shall be

processed separately for each individual telephone number or other identifier shown in the request. The names of the files transmitted shall have a structure consistent with the naming convention referred to in the Schedule.

(7) The file shall open with a single head and shall have a rigid structure provided for the particular type of network or service or the type of request. Each line in the file shall be ordered chronologically, unless another classification parameter is specified in the request. A listing pursuant to paragraph (5) shall be concluded on the last line with the word "End".

(8) In each line, individual data shall be separated by a semicolon (code 0059 of the character set) or a tabulator (code 0009 of the character set); the final datum shall end with the CRLF character (codes 0013 and 0010 of the character set). Should any of the data not be requested, or should any data demonstrably not be ascertainable from the technology used, their place in the structure shall be left blank.

(9) In respect of data consisting of multiple values, the individual values shall be separated by the "|" character (code 0166 of the character set). If the data transmitted include a character identical to any of the above separators or the "\" character (code 0092 of the character set), the "\" character shall be prepended before that character (for example, "\;", "\CR\LF", "\\").

(10) In justified cases and with the approval of the authorised authority and the operator, a format, structure and filename different from those defined in paragraphs (6) to (9) may be applied.

Section 4
Periods for the retention of data

(1) Data shall be retained for six months, unless otherwise provided in paragraph (2).

(2) The data referred to in Part 3, points 3.3.4.5 and 3.3.4.6 of the Schedule shall be retained for three months.

Section 5
Effect

This Decree shall enter into effect on the date of promulgation hereof, apart from Section 4(2) and Part 3 of the Schedule, which shall enter into effect on 1 December 2006..

Minister:
Bérová, m.p.

_____

1) Section 11 of Act No 227/2000 on electronic signatures, as amended.

VI.
Question referred

25. First, the Constitutional Court had to consider the application submitted by the applicants for it to refer a question to the European Court of Justice for a preliminary ruling in accordance with Article 234 of the EC Treaty concerning the (in)validity of the Data Retention Directive itself, since there is a significant risk that the Data Retention Directive itself, which was transposed into Czech law by means of the contested provisions and the contested Decree, is in conflict with EC law. In this respect, the Constitutional Court emphasises that, following the Czech Republic's accession to the EU (as of 1 May 2004), the constitutional norms of the Czech Republic remain the frame of reference for reviews by the Constitutional Court because the role of the Constitutional Court is to protect constitutionality (Article 83 of the Constitution of the Czech Republic) in both of its aspects, i.e. to protect

objective constitutional law and subjective (i.e. fundamental) rights. Community law is not part of the constitutional architecture and therefore the Constitutional Court is not competent to interpret that law. However, the Constitutional Court cannot entirely disregard the impact of Community law on the creation, application and interpretation of national law in terms of legislation whose creation, impact and purpose is directly linked to Community law [in this respect, see Findings of the Constitutional Court Pl. ÚS 50/04 of 8 March 2006 (N 50/40 SbNU 443; 154/2006 Sb.), Pl. ÚS 36/05 of 16 January 2007 (N 8/44 SbNU 83; 57/2007 Sb.) or II. ÚS 1009/08 of 8 January 2009 (N 6/52 SbNU 57)]. Nevertheless, the content of the Data Retention Directive itself leaves the Czech Republic sufficient room to transpose it into national in a manner consistent with the Constitution as its individual provisions essentially only define the obligation to retain data. In the transposition process, the purpose pursued by the Directive must be respected; however, in specific primary and secondary legislation on the retention and handling of data, including measures to prevent data abuse, it is necessary to adhere to the constitutional standard arising from the Czech constitutional order, as interpreted by the Czech Constitutional Court. This is because the specific form of transposition (i.e. the contested provisions of primary and secondary legislation) is a manifestation of the will of the Czech legislature, which, while respecting the purpose of the Directive, could have selected from various means, yet was bound by the constitutional order in this selection.

VII.
Terms of reference for the assessment of the application

VII. A) The right to respect for private life and the right to informational self-determination

26. Article 1(1) of the Constitution of the Czech Republic contains the normative principle of democratic rule of law. The key attribute of the constitutional concept of the rule of law and a condition for its functioning is respect for the fundamental rights and freedoms of the individual, which, as an attribute of the selected constitutional concept of the rule of law, is explicitly expressed in the cited constitutional provision. This constitutional provision is the kernel of substantively grasped legal statehood, characterised by public authority's respect for the free (autonomous) sphere of the individual, defined by fundamental rights and freedoms; as a matter of principle, public authority does not intervene in this sphere except in cases justified by conflict with other fundamental rights or constitutionally approbated public interests clearly defined by law, where it is assumed that the law anticipates intervention proportional to the objectives to be achieved and to the level to which a fundamental right or freedom is to be curtailed.

27. The concept of privacy tends to be associated most commonly with Western culture, or, more precisely, with an Anglo-American cultural concept embedded in the political philosophy of liberalism. It is a concept that apparently is not universally united in terms of its accent on the importance of privacy and the scope of what is to be protected by privacy. In different cultures, there are different ideas about the degree of privacy to which individuals are entitled and in what contexts. However, as early as 1928, Judge Brandeis wrote the following assessment of privacy in his subsequently widely cited dissent (in the case of Olmstead v US 438, 478, 1928): *"The makers of our Constitution undertook to secure conditions favourable to the pursuit of happiness (...)They conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilised men."* And it was thus that the right to privacy, not explicitly mentioned

by the US Constitution, gradually become a basic structural element of the Constitution, guaranteeing the autonomy of the individual, although battles on its application are constantly and repeatedly waged within the US Supreme Court.

28. The requirement of respect for an independent way of life became, alongside the requirement of respect for one's own life, physical, psychological and spiritual integrity, personal freedom and property rights, a central entitlement, under human rights, to the autonomy of the individual, which carries formal significance for European national catalogues of human (fundamental) rights and for their future regional and universal counterparts. Yet not even Europe's original national catalogues of fundamental rights explicitly mentioned the right to privacy or private life as such, as evidenced by the texts of national constitutions from the 1940s and 1950s (e.g. the constitutions of Germany, let alone Austria, the constitution of Denmark, Finland, and of course France, as well as Ireland, Italy and other countries). The requirements of respect for privacy and the protection thereof are closely linked to the development of technical and technological capacities, which naturally increase a country's potential to compromise freedom.

29. As the Constitutional Court notes in Finding II. ÚS 2048/09 of 2 November 2009 (available in the electronic database of decisions at http://nalus.usoud.cz): "*the fundamental right to unimpeded private life enjoys very special respect and protection in liberal democratic states (Article 10(2) of the Charter).*" The primary function of the right to respect for private life is to provide space for the development and self-realisation of individual personality. In addition to the traditional definition of privacy in its spatial dimension (the protection of the home in the broader sense) and in connection with autonomous existence and the creation of social relationships uninterrupted by public authority (in marriage, family and society), the right to respect for private life includes the guarantee of self-determination in the sense of the individual's fundamental decision-making as regards his own person. In other words, the right to privacy also guarantees the right of the individual to take decisions at his own discretion as to whether, to what extent, how and under what circumstances facts and information on his personal privacy are to be made available to other entities. This is an aspect of privacy as the right to informational self-determination, explicitly guaranteed by Article 10(3) of the Charter [cf. Constitutional Court Findings IV. ÚS 23/05 of 17 July 2007 (N 111/46 SbNU 41) or I. ÚS 705/06 of 1 December 2008 (N 207/51 SbNU 577), or Decisions of the *Bundesverfassungsgericht* BVerfGE 65, 1 (*Volkszählungsurteil*) of 15 December 1983 and BVerfGE 115, 320 (*Rasterfahndungurteil II*) of 4 April 2006].

30. In the quoted decision BVerfGE 65, 1, the *Bundesverfassungsgericht*, in assessing the constitutionality of legislation on the process of collecting and retaining data for a census (*Volkszählung*), noted that in modern society, characterised by a huge increase in information and data must, the protection of the individual from the unlimited collection, retention, use and disclosure of data about his person and privacy must be provided in the context of a broader, constitutionally guaranteed right of the individual to privacy. If an individual is not guaranteed the opportunity to monitor and control the content and scope of personal data and information provided by him, which is to be disclosed, retained or used for purposes other than the original purpose, and if the individual does not have the opportunity to identify and evaluate the credibility of a potential communication partner and adapt his conduct accordingly, then his rights and freedoms are necessarily restricted, even suppressed, and therefore there can no longer be any talk of a free and democratic society. The right to informational self-determination (*informationelle Selbstbestimmung*) is thus a prerequisite not only for the free development and self-realisation of the individual in society, but also for the

establishment of a free and democratic order of communication. Put simply, in the conditions of an omniscient and omnipresent State and public authority, freedom of expression, the right to privacy and the right to free choice of behaviour and action become virtually non-existent and illusory.

31. In the Charter, the right to respect for private life is not guaranteed in one all-encompassing article (as is the case with Article 8 of the Convention). On the contrary, the protection of an individual's private sphere is spread out over the Charter and supplemented by other aspects of the right to privacy, declared at various places in the Charter (e.g. Article 7(1) and Articles 10, 12 and 13 of the Charter). Similarly, the right to informational self-determination can be inferred from Article 10(3) of the Charter, guaranteeing the individual the right to protection from the unauthorised collection, disclosure or other misuse of his personal data, in conjunction with Article 13 of the Charter, protecting the confidentiality of correspondence and the secrecy of messages conveyed, whether kept privately or sent by post, transmitted by telephone, telegraph or other similar device, or by other means. However, this "fragmentation" of the legal regulation of individual aspects of the individual's private sphere cannot be overstated; in the Charter, the list of what is to be subsumed under the "umbrella" of the right to privacy and to private life cannot be considered exhaustive and final. In the interpretation of individual fundamental rights capturing the right of privacy in its various dimensions, as set out by the Charter, it is necessary to respect the purpose of the commonly understood and dynamically evolving right to privacy as such, i.e. the right to private life must be considered in its contemporary entirety. Therefore, the right to informational self-determination, guaranteed by Article 10(3) and Article 13 of the Charter, should also be interpreted in particular in connection with the rights guaranteed by Articles 7, 8, 10 and 12 of the Charter. By its nature and importance, the right to informational self-determination is one of the fundamental human rights and freedoms because, along with personal freedom, freedom in a spatial dimension (the home), freedom of communication and, no doubt, other constitutionally guaranteed fundamental rights, it shapes the individual's personal sphere, the individual integrity of which, as a prerequisite for the dignified existence of the individual and the development of human life in general, must be respected and rigorously protected; therefore, the respect and protection of this sphere is quite rightly guaranteed by the constitutional order because (considered from a somewhat different angle) it is an expression of respect for the rights and freedoms of man and the citizen (Article 1 of the Czech Constitution).

32. It clearly follows from the settled case-law of the Constitutional Court, particularly in relation to the interception of telephone calls, that the protection of the right to respect for private life, in the form of the right to informational self-determination within the meaning of Article 10(3) and Article 13 of the Charter, applies not only to the actual content of messages conveyed by telephone, but also to data on the numbers dialled, the dates and times of calls, their duration, and, in the case of mobile telephony, the base stations used to make the call [cf. e.g. Finding II. ÚS 502/2000 of 22 January 2001 (N 11/21 SbNU 83) – "*The privacy of every person is worthy of fundamental (constitutional) protection not only in relation to the actual content of messages conveyed, but also in relation to the data mentioned above. It is therefore clear that Article 13 of the Charter also establishes the protection of the secrecy of numbers dialled and other related information, such as the date and time of the call, its duration, and, in the case of mobile telephone calls, a specification of the base stations used to make the call. (...) such data are an integral part of communication made by telephone"* – or the similar Findings IV. ÚS 78/01 of 27 August 2001 (N 123/23 SbNU 197), I. ÚS 191/05 of 13

September 2006 (N 161/42 SbNU 327) and II. ÚS 789/06 of 27 September 2007 (N 150/46 SbNU 489)].

33. In the cited findings, the Constitutional Court also referred to ECHR case-law [in particular the decision in *Malone versus UK* (No 8691/79 of 2 August 1984)], which, from Article 8 of the Convention, guaranteeing the right to respect for private and family life, the home and correspondence, inferred the right to informational self-determination, emphasising repeatedly that collecting and retaining data on an individual's private life falls under the purview of Article 8 of the Convention because the word "private life" should not be interpreted restrictively. This facet of the right to privacy thus also encompasses the right to protection from surveillance, monitoring and harassment by public authority, even in public areas or in publicly accessible places. In addition, there is no fundamental reason allowing professional, business or social activities to be excluded from the concept of private life [cf. the judgment in Niemietz versus Germany (No 13710/88) of 16 December 1992]. As noted by the ECHR, this broad interpretation of the term "private life" is in conformity with the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (prepared by the Council of Europe as at 28 January 1981, in force in the Czech Republic as of 1 November 2001, published under number 115/2001 in the Collection of International Treaties), the purpose of which is "*to secure in the territory of each Party for every individual (...) respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), where such data are defined as "any information relating to an identified or identifiable individual" (Article 2)* [cf. the judgment in Amman versus Switzerland (No 27798/95) of 16 February 2000 and the case-law cited therein].

34. In its case-law on the right to respect for private life under Article 8 of the Convention, the ECHR indicated that interference in the privacy of individuals includes interventions in the form of data verification, the content of mail and the interception of telephone calls [cf. the judgment in *Klass and others versus Germany* (No 5029/71) of 6 September 1978, the judgment in *Leander versus Sweden* (No 9248/81) of 26 March 1987, the judgment in *Kruslin versus France* (No 11801/85) of 24 April 1990, and the judgment in *Kopp versus Switzerland* (No 23224/94) of 25 March 1998], the identifying of the telephone numbers of callers [cf. the judgment in *P G and J H versus UK* (No 44787/98) of 25 September 2001], the identifying of data about telephone connections (cf. the cited judgment in *Amman versus Switzerland*) and the retention of data on the DNA of individuals in databases of accused persons [cf. the judgment in *S and Marper versus UK* (No 30562/04 and 30566/04) of 4 December 2008]. In the judgment in *Rotaru versus Romania* (No 28341/95) of 4 May 2000, the ECHR concluded, by reference to the right to private life as manifested in the form of the right to informational self-determination, that the State had the positive obligation to destroy data that had been collected and processed on a person from his private sphere.

35. A similar approach is taken in the case-law of foreign constitutional courts. For example, Germany's *Bundesverfassungsgericht, via* the right to informational self-determination, guarantees the protection not only of the content of communications, but also of the external circumstances under which they take place, i.e. the location, time, participants, type and method of communication, because knowledge of the circumstances underlying communications may, in conjunction with other data, indicate the content of communication and may make it possible, subject to exploration and analysis of such data, to draw up individual profiles of the participants in the communication [cf. e.g. the judgments of 27 July

2005, BVerfGE 113, 348 (*Vorbeugende Telekommunikationsüberwachung*) and 27 February 2008, BVerfGE 120, 274 (*Grundrecht auf Computerschutz*).

VII. B) The admissibility of interference with the right to informational self-determination

36. Protection from security threats and the need to ensure the availability of data for the prevention, detection, investigation and prosecution of serious criminal offences by public authorities are commonly cited as a primary goal of legal regulation concerning the blanket and preventive collection and retention of traffic and location data on electronic communications. As the Constitutional Court repeatedly stressed in the past, the prosecution of criminal offences and the punishment of offenders is constitutionally approbated by the public interest, the essence of which is the transfer of responsibility for prosecuting the most serious violations of fundamental rights and freedoms by natural persons and legal persons to the State. Where criminal law facilitates the realisation of the public interest in prosecuting crimes by means of robust tools, the use of which results in severe restrictions on personal integrity and fundamental rights and freedoms of the individual, constitutional limits must be respected in their application. The restriction of personal integrity and personal privacy (i.e. the breaking of respect for them) by public authority may therefore only occur in exceptional circumstances necessitated in a democratic society, provided that the objective pursued by the public interest cannot be achieved otherwise and if this is acceptable in terms of the legal existence and observance of effective and specific guarantees against arbitrariness. Essential prerequisites of a fair trial require an individual to be endowed with sufficient guarantees and safeguards against possible abuse of power by public authorities. Those necessary guarantees consist of the corresponding legislation and the existence of effective monitoring of observance thereof, primarily comprising checks on the most intensive interferences with fundamental rights and freedoms of individuals by an independent and impartial court, because it is the duty of the courts to ensure the protection of the fundamental rights and freedoms of individuals (Article 4 of the Constitution of the Czech Republic) [cf. Findings I. ÚS 631/05 of 7 November 2006 (N 205/43 SbNU 289) and Pl. ÚS 3/09 of 8 June 2010 (219/2010 Sb., available in the electronic database of decisions at http://nalus.usoud.cz)].

37. In its case-law, the Constitutional Court defined in more detail the fulfilment of the conditions outlined above when considering the admissibility of a public authority's interference with the privacy of the individual through the use of telecommunications interception [cf. e.g. the cited Findings II. ÚS 502/2000, IV. ÚS 78/01, I. ÚS 191/05, and Finding I. ÚS 3038/07 of 29 February 2008 (N 46/48 SbNU 549)]. Interference with the individual's fundamental right to privacy, in the form of the right to informational self-determination within the meaning of Article 10(3) and Article 13 of the Charter, in order to prevent and protect against criminal activity is thus possible only through mandatory legislation which, above all, must comply with the demands arising from the rule of law and which meets the requirements of the proportionality test, where, in cases of conflict between fundamental rights and freedoms and the public interest, or other fundamental rights and freedoms, the purpose (aim) of such interference in relation to the means used must be assessed; the benchmark for this assessment is the principle of proportionality (in the broader sense). Such legislation must be precise and clear in its formulation and predictable enough to provide potentially affected individuals with sufficient information about the circumstances and conditions under which a public authority is entitled to interference with their privacy, so that, where appropriate, they can adjust their behaviour so as not to come into conflict with such restrictive provisions. The powers granted to the competent authorities, and the method

and rules for exercise thereof so that individuals are given protection against arbitrary interference, must be strictly defined. An assessment of the admissibility of interference from the perspective of the principle of proportionality (in the broader sense) encompasses three criteria. The first of these is an assessment of the capability of complying with the purpose (or expediency); it is ascertained whether a particular action is capable of achieving the intended objective of protecting another fundamental right or public good. Then there is an assessment of need, examining whether the means selected is the means most considerate in relation to the fundamental right. Finally, adequacy (in the stricter sense) is examined, i.e. whether the loss incurred in respect of a fundamental right is proportionate to the intended objective. This means that the negative ramifications of measures restricting fundamental human rights and freedoms must not, in the case of a conflict between a fundamental right or freedom and the public interest, outweigh the positives representing the public interest in these measures [cf. Finding Pl. ÚS 3/02 of 13 August 2002 (N 105/27 SbNU 177; 405/2002 Sb.)].

38. An essential requirement for the judicial protection of fundamental rights, in the event of the application of criminal-law instruments restricting the fundamental rights and freedoms of the individual, lies, in particular, in the issue of a court order and its sufficient justification. This must correspond to the requirements of the law and, especially, the constitutional principles on which the law is based, or which limit its interpretation, as the application of such provisions constitutes particularly serious interference with the fundamental rights and freedoms of any individual. "*A court order for the interception and recording of telecommunications traffic may be issued only in duly instituted criminal proceedings for legally classified criminal activity, and must be supported by relevant indications, from which a reasonable suspicion of such crime can be inferred. An order must be individualised to a specific person using a telephone station. Finally, an order must at least specify which facts relevant to criminal proceedings are to be ascertained, and from what this has been derived*" [cf. the cited Findings of the Constitutional Court II. ÚS 789/06 and I. ÚS 3038/07).

39. A similar approach is applied by the ECHR in its case-law. Therefore, the ECHR, in accordance with Article 8(2) of the Convention, which defines the constitutional limits of restrictions on fundamental rights and freedoms of individuals guaranteed by Article 8(1) of the Convention, considers as a matter of priority, in each case, whether the alleged interference with or restriction on fundamental rights or freedoms can be subsumed under the scope of protection offered by Article 8 of the Convention. If it can, whether the alleged interference with the right to privacy by a public authority was made in accordance with the law, which must be accessible and sufficiently foreseeable, i.e. expressed with a high degree of accuracy so as to allow individuals, if necessary, to regulate their behaviour (cf. *Malone versus UK*, *Amman versus Switzerland* and *Rotaru versus Romania*). The level of accuracy required by national legislation, which cannot be prepared for all eventualities, depends to a large extent on the content of the text examined, on the area to be covered, and on the number and status of persons to whom it is addressed [*Hassan and Tchaouch versus Bulgaria* (No 30985/96, 39023/97 of 26 October 2000]. Interference with fundamental rights or freedoms guaranteed by Article 8(1) of the Convention must, within the meaning of Article 8(2) of the Convention, also be necessary in a democratic society, pursue an objective approbated by the Convention (e.g. the protection of human life or health, national and public security, the protection of the rights and freedoms of others or morals, the prevention of disorder or crime, or an interest in the economic prosperity of the country), which must be relevant and duly justified. In order for statutory provisions to be assessed as conforming to the Convention, they must, within the meaning of Article 13 of the Convention, also provide adequate protection from arbitrariness and, consequently, define with sufficient clarity the scope and

manner for the exercise of powers conferred on the competent authorities (cf. *Kruslin versus France* and *S and Marper versus UK*). In other words, the actions constituting obvious interference with the fundamental right to private life must not be outside the realm of any direct (preventive or post-) judicial control [cf. the judgment in *Camenzind versus Switzerland* (No 21353/93) of 16 December 1997].

40. The requirements of legislation facilitating interference with the right to private life, as mentioned by the ECHR, are defined in more detail in the above-mentioned judgments, in which it assessed the validity of such interference by public authorities through the interception of telephone calls, secret surveillance, and the collection of information and data from the private (personal) sphere of the individual. The ECHR pointed out that, first, it is necessary to establish clear and detailed rules governing the scope and application of such measures, set the minimum duration requirements, the method for retaining the information and data, their use, and third-party access thereto, and establish procedures to protect the integrity and confidentiality of data and to destroy them in such a way that individuals are given sufficient guarantees that their data will not be subject to the risk of abuse and arbitrariness. The need to wield such guarantees is even greater as regards the protection of personal data subjected to automatic processing, particularly if these data are used for police objectives or in a situation where the available technology is becoming increasingly sophisticated. National law must, in particular, ensure that collected data are genuinely relevant and not excessive in relation to the purpose for which they were secured, and that they are kept in a form which enables the identification of persons for a period not exceeding the necessary extent to achieve the purpose for which they were secured [cf. the Preamble and Article 5 of the Convention on Data Protection and Principle 7 of Recommendation No R(87)15 of the Committee of Ministers of 17 September 1987 relating to the regulation and use of personal data in the police sector, cited according to the judgment in *Weber and Saravia versus Germany* (No 54934/00) of 29 June 2006 and *Liberty and others versus UK* (No 58243/00) of 1 July 2008].

VIII. Actual review

VIII. A) Data retention

41. As mentioned above by the Constitutional Court, the contested provisions of Section 97(3) and (4) became part of Act No 127/2005 on electronic communications on the basis of Act No 247/2008 amending Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended. According to the explanatory memorandum, this amendment was adopted to transpose "certain articles" of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC "*which had not previously been implemented in Czech law, or have been implemented only partially (as) the Data Retention Directive has already been transposed in the Czech Republic (...). In some respects, legislation in force is broader than that contained in the Data Retention Directive.*" The issue of the retention of traffic and location data has been regulated, in a modified form, in the Czech legal system since the adoption of Act No 127/2005 on electronic communications, with effect as of 1 May 2005, and since the adoption of the contested Decree of the Ministry of Informatics No 485/2005 on the scope of traffic and location data, the period of retention thereof, and the form and method

of transmission thereof to bodies authorised to use them, with effect as of 15 December 2005. At that time, the EU was still preparing the Data Retention Directive. Therefore, it was effectively implemented in the Czech Republic in advance, and the actual wording of the contested provisions, pursuant to the requirements of the Data Retention Directive, merely serve to clarify the obligation to retain traffic and location data and to provide such data to authorised bodies promptly upon request. Nevertheless, the contested Decree of the Ministry of Informatics, despite this fact, has not been amended, resulting in a situation where the scope of the data retained, as regulated by the contested legislation, remains clearly above the framework of the scope anticipated by the Data Retention Directive.

42. According to the contested Section 97(3), first and second sentences, of the Electronic Communications Act, a legal or natural person providing a public communications network or providing a publicly available electronic communications service shall retain traffic and location data which are generated or processed in the provision of its public communications networks and in the provision of its publicly available electronic communications services, including data on unsuccessful call attempts, where such data are generated or processed, and also retained or recorded. Under Section 90 of the Electronic Communications Act, traffic data means *"any data processed with a view to the transmission of a message via an electronic communications network or for the accounting thereof."* Under Section 91 of the same Act, location data means *"any data processed in an electronic communications network which identify the geographic location of the terminal equipment of a user of a publicly available electronic communications service."* An implementing regulation, i.e. the contested Decree No 485/2005, should define the specific nature and scope of traffic and location data, the period of retention thereof, and the form and method of transmission thereof to bodies authorised to use them under Section 97(4).

43. Specifically with fixed telephony and mobile communications, operators are obliged to collect virtually all available data on calls made and (if recorded) on unsuccessful call attempts (typically a "ring"). In particular, these are data of on the underlying form of communication, on the telephone numbers of the caller and the person called, on the date and time of communication commencement and termination, a specification of the base station providing the call at the moment of connection, the identification of prepaid telephone cards, public payphones, and, in the case of mobile communications, also data on the unique code used to identify each mobile telephone used in the GSM network (IMEI), its location and movement, even in the absence of any communication (it is enough for the mobile telephone to be switched on) the numbers of recharging coupons and the matching thereof with the number recharged, the link between a mobile device and any SIM cards inserted, etc. An even greater volume and scope of data which, according to the contested legislation, must be retained exists in relation to public networks functioning on the principle of packet switching and services, most typically the Internet. If applied, the contested legislation requires the retention of data primarily concerning access to the network (e.g. the time, place and length of the connection, information about users and user accounts, the identifier of the computer and server accessed, the IP address, the full domain name, the volume of data transmitted, etc.), as well as data related to access to e-mail boxes and the transmission of electronic mail messages (in this case virtually all data except the content of the messages themselves, i.e. including the identification of addresses, the amount of traffic, etc., are retained). Not least, data on server and other services [e.g. the URL addresses entered, the type of request, information on the use of chat, usenet, instant messaging (e.g. ICQ) and IP telephony, including the identification of the communicating parties, the time and the services used (such as file transfer or transactions)] are retained. Beyond the scope of the Data Retention Directive, in relation to

Internet connections and services and e-mail communications, the quantity of data transmitted, information on the use of encryption, the method and status of requests for services and implementation thereof, as well as information on the sending of SMS messages from Internet gateways and others "interest identifiers" are monitored and retained. In the case of telephony, beyond the Data Retention Directive the contested legislation requires the retention of data on the identification of prepaid telephone cards, public payphones, the numbers of recharging coupons and the matching thereof to the number recharged, and links between a mobile device and the SIM cards inserted.

44. Although the obligation to retain traffic and location data does not apply to the content of individual communications (see Article 1(2) of the Data Retention Directive and the contested provision of Section 97(3), fourth sentence), it is possible, by combining data about users, addressees, the exact times, dates, places and forms of telecommunication connections, if monitored over an extended period of time, to compile detailed information about social or political affiliation, as well as about the personal hobbies, inclinations or weaknesses of individual persons. In the Senate's statement summarised above, the view put forward by the submitter of the bill that "*in no way can this be likened to tapping, if only because the content of individual calls or email messages is not stored*" is entirely wrong because even this basis is enough to make sufficient content-related conclusions falling within the private (personal) sphere of the individual. Based on these data, it is possible to infer, with up to 90% certainty, with whom, how often, and even at what hours an individual is in contact, who his closest acquaintances, friends or colleagues from work are, or what activities he is involved in and at what times of day [cf. a study by the Massachusetts Institute of Technology (MIT), Relationship Inference, available at http://reality.media.mit.edu/dyads.php]. The collection and retention of location and traffic data therefore also constitutes significant interference with the right to privacy and as such it is necessary, within the scope of the protection of the fundamental right to respect for private life, in the form of the right to informational self-determination (as defined in Article 10(3) and Article 13 of the Charter), to include not only the protection of the actual content of messages conveyed by telephone communication or communication via the so-called public networks, but also the traffic and location data about such messages.

VIII. B) Assessment of the contested legislation in terms of constitutional requirements

45. Constitutional Court had to consider whether the contested legislation, which regulates the blanket and preventive collection and retention of specified traffic and location data on electronic communications ("data retention"), is consistent with the outlined constitutional requirements as regards legislation enabling interference with the fundamental rights of individuals to privacy in the form of the right to informational self-determination (as defined in Article 10(3) and Article 13 of the Charter). Furthermore, with respect to the intensity of such interference, which in this case is highlighted by the fact that it affects a huge number and unpredictable of participants in communication, as it concerns the blanket and preventive collection and retention of relevant data, it the most stringent possible benchmarks had to be imposed on the fulfilment of the above requirements. The Constitutional Court concluded that, for several reasons, the contested legislation fell far short of the constitutional requirements outlined above.

46. The contested provisions of Section 97(3), third sentence, of the Electronic Communications Act only vaguely and entirely indistinctly impose the obligation on legal or

natural persons retaining traffic and location data in the above range "*to provide them, on request, to authorities authorised to request them pursuant to special legislation*." Although contested Decree specifies, in Section 3, how this obligation is to be met in relation to the authorised authorities in individual cases, i.e. it defines in relatively great detail the data transmission method, the communication method (electronic), the format, the programs used, codes, etc., in the Constitutional Court's view it is not clear from the actual wording of the contested provisions of Section 97(3) of the Electronic Communications Act or from the explanatory memorandum which authorised authorities and which special legislation are specifically concerned. With regard to wording of Section 97(1) of the Electronic Communications Act, which requires legal or natural persons providing a public communications network or providing a publicly available electronic communications service to set and run, at the expense of the requesting party, interfaces at designated points on their network for the connection of terminal telecommunications equipment for the interception and recording of messages, one can only assume that the obligation to forward retained traffic and location data concerns the same authorised authorities and similar special legislation addressed to law enforcement agencies, evidently according to Section 88a of the Criminal Code, the Security Information Service, according to Sections 6 to 8a of Act No 154/1994 on the Security Information Service, and Military Intelligence, according to Sections 9 and 10 of Act No 289/2005 on Military Intelligence. The legislation thus defined, enabling large-scale interference with fundamental rights, does not meet the requirements of certainty and clarity in terms of the rule of law (see paragraph 37).

47. Nor is there a clear and precise definition of the purpose for which the traffic and location data are to be provided to authorised authorities, making it impossible to assess the contested legislation with regard to actual needs (whether it is capable of meeting the purpose or fulfilling the objective set by the Directive – see below). While the cited Data Retention Directive clearly states in Article 1(1) that it aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of traffic and location data required to identify a subscriber or registered user in order to "*ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime*" (although it does not specify what sort of crime this is), no such restriction is included in the contested legislation or the cited provisions of Section 88a(1) of the Criminal Code, governing conditions for the use of retained data for purposes of criminal proceedings. The legislature has not linked the possibility of using retained data in criminal proceedings, according to the legislation in question, to the reasonable suspicion of a serious crime. Furthermore, there is no obligation for law enforcement agencies to notify this fact to the person concerned (the person under surveillance), even subsequently. Therefore, this legislation fails to meet the requirements arising from the second step of the proportionality test, i.e. necessity in the selection of means, because it is clear from the above that the means most considerate to the fundamental right to informational self-determination has not been applied.

48. The Constitutional Court regards as inadequate and unforeseeable this method of (not) defining the range of authorised public authorities, as well as the (non-)definition of the purpose for which they are entitled to request the retained data. Although, according to the cited Section 88a(1) of the Criminal Code, the use of retained data is subject to judicial control in the form of authorisation issued by the presiding judge (and in pre-trial procedure by a judge), it was primarily the duty of the legislature to set more clearly and unambiguously the requirements and conditions for the use of retained data and the scope of application

thereof in the contested provisions or in the cited Section 88a(1) of the Criminal Code, rather than the completely vague definition of conditions for the use of data retained "*on the realisation of telecommunications traffic" in order to* "*clarify facts relevant to criminal proceedings*". In particular, it is necessary, in view of the seriousness and the degree of interference with the fundamental right of individuals to privacy in the form of the right to informational self-determination (as defined in Article 10(3) and Article 13 of the Charter), setting out the use of retained data, for the legislature to limit opportunities for the use of retained data solely for the purposes of criminal proceedings concerning particularly serious crimes, and even then only in cases where it is impossible to achieve the objective pursued by other means. Moreover, this is anticipated not only by the Data Retention Directive, but also by Section 88(1) of the Criminal Code, governing conditions under which the interception and recording of telecommunications traffic may be ordered ("*if criminal proceedings are held in respect of a particularly serious crime*"), from which the provisions of Section 88a of the Criminal Code as a whole (despite the legal opinions of the Constitutional Court contained in the cited Findings II. ÚS 502/2000 and IV. ÚS 78/01) derogates entirely without reason, instead laying down provisions which clearly contrast with the Constitutional Court's opinions.

49. The absence of proper legislation (i.e. legislation conforming to the Constitution), as is clear from statistical data, results in practice in a situation where this instrument, in the form of requests for and the use of retained data (including data on calls not connected, which are not covered by the Criminal Code), is used (and abused) by law enforcement agencies even for the purposes of investigating petty (less serious) crime. For example, according to the "*Report on the Security Situation in the Czech Republic 2008*", a total of 343,799 crimes were detected in the Czech Republic, of which 127,906 were solved. In the same period, the number of requests for traffic and location data by authorised public authorities came to 131,560 [cf. the European Commission's report "*The Evaluation of Directive 2006/24/EC and National Measures to Combat the Criminal Misuse and Anonymous Use of Electronic Data*", which sought official figures from the Czech Republic - the responses by representatives of the Czech Republic to the questions in the questionnaire of 30 September 2009 are available at http://www.dataretention2010.net/docs.jsp). Consequently, and not only for the period from January to October 2009, unofficial figures indicate that requests for location and traffic data were made in 121,839 cases (cf. Herczeg, J: *Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou*, Bulletin advokacie 5/2010, p. 29).

50. In the Constitutional Court's view, the legislation contested by the applicants also quite inadequately (if at all) establishes clear and detailed rules laying down minimum requirements designed to keep retained data secure, in particular by preventing third-party access and setting out procedures to protect the integrity and confidentiality of data, as well as data destruction procedures. The contested legislation should also be criticised for failing to provide the individuals concerned with sufficient guarantees that their data would not be at risk of abuse and arbitrariness. Today, the need for such guarantees is all the more urgent for individuals in the present case concerning the blanket and preventive collection and retention of data in electronic communications of individuals because the enormous development and occurrence of new, more complex information technologies, systems and means of communication inevitably leads to a smooth shift in the boundaries between private and public space in favour of the latter. This is because, in the virtual space of information technology and electronic communications ("cyberspace"), thousands – even millions – of pieces of data and information are collected and effectively made available every minute

(thanks to the development of the Internet and mobile communications) which interfere with the private (personal) sphere of all individuals, even though they do not consciously want to let anyone into that sphere.

51. The Constitutional Court does not regard as sufficiently clear, detailed and adequate guarantees the mere enshrinement of the obligation imposed on legal or natural persons to ensure "*that the content of messages is not stored together with the defined retained data*" (Section 97(3), fourth sentence), or the obligation to "*destroy them upon expiry of the period, unless such data have been provided to authorities authorised to request them under special legislation or unless otherwise provided by the present Act (Section 90)*" (Section 97(3), sixth sentence). The definition of the period of retention, i.e. "*not less than six months and not more than 12 months*", the expiry of which gives rise to the obligation to destroy the data, is ambiguous and, considering the scale and sensitivity of the data retained, woefully inadequate. For none of these obligations do detailed rules and specific procedures for their implementation exist. There are no strictly defined requirements for the security of the data retained. The way the data are handled, either by the legal or natural persons retaining the traffic and location data, or, following a request, by authorised public authorities, is not sufficiently ascertainable, nor is a specific means of data destruction established. Likewise, there is no definition of responsibilities or penalties for failure to comply with such obligations, including the absence of the possibility for the individuals concerned to seek effective protection from abuse, arbitrariness, or con-compliance with set obligations. Oversight by the Office for Data Personal Protection "*of compliance with obligations in the processing of personal data*", as anticipated by the Electronic Communications Act (Section 87 et seq.), and the instruments defined for that Office's activities and checks, cannot be regarded as an adequate and effective means to protect the fundamental rights of the individuals concerned because they do not control this instrument themselves [see, mutatis mutandis, Finding Pl. ÚS 15/01 of 31 October 2001 (N 164/24 SbNU 201; 424/2001 Sb.)]. As a result of inadequate legislation inconsistent with the constitutional requirements above, these acts, constituting obvious interference with the fundamental right of individuals to privacy in the form of the right to informational self-determination (as defined in Article 10(3) and Article 13 of the Charter), find themselves bereft of any immediate (even follow-up) control, especially judicial control, the need for which was expressed by the ECHR in the cited judgment in Camenzind versus Switzerland.

52. Similar conclusions have been reached by constitutional courts in other European countries, which also reviewed the constitutionality of legislation implementing the Data Retention Directive. For example, the *Bundesverfassungsgericht, in* judgment 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 of 2 March 2010, found that the contested legislation governing the preventive retention of data (*Vorratsdatenspeicherung*) (within the meaning of Sections 113a, 113b of the *Telekommunikationsgesetz*) and their use in criminal proceedings (within the meaning of Section 100g(1) of the *Strafprozessordnung*) was unconstitutional due to inconsistency with Article 10(1) of the *Grundgesetz*, which guarantees the inviolability of correspondence, postal and telecommunications secrecy. The *Bundesverfassungsgericht* held that the contested legislation does not satisfy the requirements arising from the principle of proportionality, which requires, among other things, that legislation on data retention reflect the specific gravity of such an interference with the fundamental rights of individuals. Specifically, the contested legislation insufficiently defined the purpose of using such data, failed to guarantee them adequate security and, not least, did not guarantee individuals adequate and effective safeguards against the risk of abuse, especially in the form of judicial control. Pursuant to Article 73(1)(7) of the *Grundgesetz*, the federal legislature was called on

to meet these requirements. Similar conclusions were reached by the Romanian *Curtea Constituțională* in its judgment of 8 October 2009 (No 1258), which labelled the local legislation as unconstitutional as it failed to define the purpose of use of such a tool, its wording was too vague, without defining in detail the powers and duties authorised public authorities, and, in the absence of judicial control, individuals were not given sufficient guarantees against abuse (this judgment is available in an unofficial English translation at http://www.legi-internet.ro/english/jurisprudenta-it-romania/decisii-it/romanian constitutional-court-decision-regarding-data-retention.html), as well as by the Supreme Administrative Court of Bulgaria in a judgment of 11 December 2008 (information available at http://www.edri.org/edri-gram/number6.24/Bulgarian-administrative-case-data-retention) and the Supreme Court of Cyprus in a judgment of 1 February 2011 (information at http://www.edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus). Moreover, the Constitutional Court has discovered that legislation implementing the Data Retention Directive is currently under review in Poland and Hungary. The need to ensure the most stringent safeguards and instruments to protect the fundamental rights of individuals in the handling their personal data from electronic communications was also stressed by the European Court of Justice in its decision in preliminary ruling procedure of 9 November 2010 in the Joined Cases of *Volker und Markus Scheck GbR GbR and Hartmut Eifert versus Land Hessen* (C-92/09 and C-93/09).

53. In view of the foregoing, the Constitutional Court observes that the contested provisions of Section 97(3) and (4) of Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended, and the contested Decree No 485/2005 on the scope of traffic and location data, the period of retention thereof, and the form and method of transmission thereof to bodies authorised to use them cannot be considered constitutional because they clearly violate the constitutional limits outlined above in that they fail to meet demands stemming from the principle of the rule of law and are in conflict with requirements regarding the limitation of the fundamental right to privacy in the form of the right to informational self-determination within the meaning of Article 10(3) and Article 13 of the Charter, which have their basis in the principle of proportionality.

54. Beyond that, the Constitutional Court considers it necessary to point out that the above deficiencies, which led to the derogation of the contested legislation, are not even respected by special laws on which the contested provision of Section 97(3) of the Electronic Communications Act was indirectly relying. In the opinion of the Constitutional Court, the cited provisions of Section 88a of the Criminal Code, governing conditions for the use of retained data on telecommunications traffic for purposes of criminal proceedings, in particular by no means respects constitutional limits and requirements outlined above, and as such also appears to be unconstitutional to the Constitutional Court. However, as it was not contested by the applicants in their application, the Constitutional Court considers it necessary to appeal to the legislature, as a consequence of the derogation of the contested legislation, to consider amending Section 88a of the Criminal Code too in order to align it with the Constitution.

VIII. C) Obiter dictum

55. The Constitutional Court observes, merely in the form of an obiter dictum, that it is fully aware of the fact that, hand in hand with the development of modern information technology and means of communications, new and more sophisticated forms of criminal activity are emerging which need to be countered. Nevertheless, the Constitutional Court has doubts

about whether the blanket and preventive retention of traffic and location data on almost all electronic communications is a necessary and appropriate tool given the intensity of its interference with the private sphere of a vast number of electronic communication users. This view is far from isolated in Europe, as, since its inception, the Data Retention Directive itself has faced a huge wave of criticism both from Member States (e.g. the governments of Ireland, the Netherlands, Austria and Sweden waited a long time before implementing it or are still holding back on its implementation, the latter two countries despite the Commission's publicly announced threat to initiate proceedings before the European Court of Justice), and from legislators in the European Parliament, the European Data Protection Supervisor (see the conclusions of the conference on data retention held by the Commission on 3 December 2010 in Brussels, http://www.dataretention2010.net/docs.jsp), the Working Party on Data Protection, established under Article 29 of Directive 95/46/EC (cf. its opinions posted on http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm), and non-governmental organisations (including Statewatch, European Digital Rights and Arbeitskreis Vorratsdatenspeicherung – AK Vorrat). All of the above have sought either the full annulment of the Data Retention Directive and the replacement of the blanket and preventive retention of traffic and location data with other, more appropriate tools (e.g. data freezing, which, if the set conditions are met, facilitates the tracking and retention of necessary, selected data only in relation to a specific, predetermined communication subscriber), or the amendment of the Data Retention Directive, especially in the form of adequate guarantees and means of protection for the individuals concerned, along with a tightening of requirements to keep the retained data secure against the threat of leaks and misuse by third parties.

56. The Constitutional Court also had doubts upon examining whether the blanket and preventive retention of traffic and location data, in terms of its original purpose (protection from security threats and the prevention of particularly serious crime), was an effective tool, especially given the existence of anonymous SIM cards, which are not included in the contested legislation on the anticipated extent of retained traffic and location data and which, according to observations by the Czech Police Force, account for up to 70% of communications used in the commission of crime (cf. "*Česká policie chce zakázat anonymní předplacené karty, operátoři se brání*" ["Czech police want to ban anonymous prepaid cards, operators resist"], iDNES.cz, 18 March 2010). In this context, we also refer to an analysis by the Federal Bureau of Investigation in Germany (the *Bundeskriminalamt*) of 26 January 2011, which, after comparing statistics on serious crimes committed in Germany in the period before and after the adoption of the legislation on data retention, arrived at the conclusion that the use of the blanket and preventive retention of traffic and location data had little effect on reducing the number of serious crimes committed or on improving the crime solving rate (the analysis and specific statistical data are available at http://www.vorratsdatenspeicherung.de/content/view/426/79/lang.de/). Similar conclusions can be made even by a cursory look at the statistical summaries of crime in the Czech Republic, as published by the Czech Police Force, e.g. a comparison of statistics for the periods 2008 to 2010 (available at http://www.policie.cz/clanek/statisticke-prehledy-kriminality-650295.aspx).

57. Finally, the Constitutional Court considers it necessary to express doubts as to whether it is desirable for private entities (providers of Internet, telephony and mobile communications services, especially mobile operators and companies providing Internet access) to be granted the power to retain all data about the communications provided by them, as well as about customers to whom their services are provided (i.e. data beyond the scope of the data which they are required to retain by the contested legislation), and to dispose of such data freely for

the purposes of recovering debts and developing their business activities and marketing operations. In the Constitutional Court's view, this is disagreeable primarily on the grounds that neither the Electronic Communications Act nor any other legislation regulates this authorisation and its purpose in detail, or offers a strict definition of rights and obligations or the scope of data to be retained, or the period and method of retention; likewise, requirements regarding data security and control mechanisms are not specified in detail.

58. Therefore, in view of the foregoing, the Constitutional Court has decided, pursuant to Section 70(1) of the Constitutional Court Act, to annul the contested provisions of Section 97(3) and (4) of Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended, and Decree No 485/2005 on the scope of traffic and location data, the period of retention thereof, and the form and method of transmission thereof to bodies authorised to use them on the date of publication of this Finding in the Collection of Laws (Section 58(1) of the Constitutional Court Act).

59. The applicability of data already requested for the purposes of criminal proceedings needs to be examined by the ordinary courts in terms of the proportionality of interference with the right to privacy in each individual case. In particular, the courts must consider the seriousness of the criminal offence in the light of facts forming the basis for the criminal proceedings in which the requested data are to be used.

Advice: No appeals may be lodged against this decision of the Constitutional Court (Section 54(2) of the Constitutional Court Act).

Brno, 22 March 2011

Pavel Rychetský
President of the Constitutional Court