Pl. ÚS 45/17 of 14 May 2019
161/2019 Sb.

Data Retention III (Collecting and Using Traffic and Location Data on the Telecommunication Traffic)

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

Under file reference Pl. ÚS 45/17 of 14 May 2019, the Constitutional Court, in the Plenum consisting of the Chairman of the Court Pavel Rychetský and Judges Ludvík David, Jaroslav Fenyk, Josef Fiala, Jan Filip, Jaromír Jirsa (Judge Rapporteur), Tomáš Lichovník, Vladimír Sládeček, Radovan Suchánek, Kateřina Šimáčková, Vojtěch Šimíček, Milada Tomková, David Uhlíř, and Jiří Zemánek, held on the petition of a group of Deputies, represented by Mgr. et Mgr. Jan Vobořil, attorney-at-law with the registered office in Prague 7, U Smaltovny 1115/32, seeking the annulment of the provisions of Section 97 (3) and (4) of Act No. 127/2005 Coll., on Electronic Communications and on Amendment to Certain Related Acts (Electronic Communications Act), as amended, Section 88a of Act No. 141/1961 Coll., on Criminal Procedure (Criminal Procedure Code), as amended, Section 68 (2) and Section 71 (a) of Act No. 273/2008 Coll., on the Police of the Czech Republic, and Decree No. 357/2012 Coll., on the retention, transmission and destruction of traffic and location data, with the participation of the Parliament of the Czech Republic and the Ministry of Industry and Trade as the parties to the proceedings and the Government as the secondary party, as follows:

The petition shall be dismissed.

Reasoning

I.

Definition of the Matter

1. In accordance with Art. 87 (1) (a) and (b) of the Constitution of the Czech Republic (hereinafter only as the "Constitution"), by means of a petition of 20/12/2017, a group of 58 Deputies (hereinafter only as the "Group of Deputies" or the "Petitioner") is seeking the annulment of the provisions specified in the heading in the proceedings before the Constitutional Court in accordance with Section 64 et al of Act No. 182/1993 Coll., on the Constitutional Court, as amended (hereinafter only as the "Constitutional Court Act").

2. The petition challenges certain provisions of the legal regulation on preventive retention of traffic and location data on electronic communications by telecommunications service providers (hereinafter only as "data retention") and the possibilities of providing them subsequently: a) to the law enforcement bodies, b) to the Police of the Czech Republic (hereinafter only as the "Police") for the purpose of an initiated search for a specific wanted or missing person, identification of a person of unknown identity or the identity of a found corpse, or prevention or detection of specific terrorist threats, c) to the Security Information Service, d) to the Military Intelligence, and e) to the Czech National Bank for the purposes of capital market supervision.

3. The contested legal regulation pursues, as is apparent from the relevant statements of reasons, various objectives which are also deductible from the list of authorities competent to handle the retained data. These include the security and defence of the state, the protection of persons and property against crime, the search for wanted, missing or lost persons, and supervision of the capital market. The original legal regulation establishing the obligation to retain traffic and location data was adopted in 2005 in response to the increasing security risks related to the increasing use of electronic communication systems, which made it necessary to adapt the powers of the authorities in charge of security and defence tasks in the Czech Republic and represented the implementation 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

(hereinafter only as the "Data Retention Directive"), on the basis of the ruling of the Court of Justice of the European Union (hereinafter only as the "CJEU"), which is no longer applicable today (see below).

4. In order to achieve the above objectives, the contested legal regulation imposes on obligated entities (providers of electronic communications services, hereinafter only as the "operators") to retain "data packages" concerning all clients, users of telecommunication services, retrospectively for a period of six months. For example, in the case of telephone calls or SMS and MMS messages (including unsuccessful connection attempts), the operator stores information about the telephone numbers of the calling and called party, the date and time of commencement and termination of the communication, and the location and movement of the user of the particular service. In the case of use of the Internet services and e-mail communication, the operators are also obliged to collect, in particular, user accounts, computer and search server IDs (the IP address or port number), information about the e-mail address of communication participants and the electronic mail protocol.

5. Simply put, under the contested legal regulation, the operators retain information on each telephone connection, text message, Internet connection or e-mail correspondence, i.e. detailed data on all communication, location of communication participants and the Internet services provided. Some of these data are stored by the operators for their own needs (billing services, complaints, or marketing) even without the obligation stipulated by the contested law.

II.

Petitioner's Arguments

6. The Group of Deputies seeks the annulment of the contested legal regulation, as it unconstitutionally interferes with the right to privacy guaranteed in Art. 7 (1) of the Charter of Fundamental Rights and Freedoms (hereinafter only as the "Charter"), the right to be protected from any unauthorised intrusion into their private and family life under Art. 10 (2) of the Charter, the right to be protected from the unauthorised gathering, public revelation, or other misuse of their personal data under Art. 10 (3) of the Charter, and the right to maintain confidentiality of communications sent by telephone, telegraph, or by other similar devices under Art. 13 of the Charter. The Petitioner also alleges that the contested provision is inconsistent with Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter only as the "Convention").

7. The Petitioner introduces its arguments by referring to the previous case law of the Constitutional Court and the Court of Justice of the European Union, which has already addressed the issue of data retention [the Judgment of the Constitutional Court file reference Pl. ÚS 24/10 of 22 March 2011 (N 52/60 SbNU 625; 94/2011 Coll.); the Judgment of the Constitutional Court file reference Pl. ÚS 24/11 of 20 December 2011 (N 217/63 SbNU 483; 43/2012 Coll.); the Judgments of the Court of Justice of the European Union of 8 April 2014 in the joined cases C-293/12 and C-594/12 (Digital Rights Ireland Ltd) and of 21 December 2016 in the joined cases C-203/15 and C-698/15 (Tele2 Sverige AB)].

8. The petition alleges, first of all, that the contested legal regulation is disproportionate in relation to the constitutionally guaranteed right to privacy, since it does not preserve its essence and meaning under Art. 4 (4) of the Charter. In the view of the Petitioner, the very monitoring, collection and retention of traffic and location data is unconstitutional, since it is blanket and non-selective. The Petitioner alleges that the measure creates a legitimate feeling that everyone is under constant supervision and does not allow any distinction. At present, much more data is being generated than in 2011, when the Constitutional Court last decided on the matter, as the use of data services in mobile ("smart") phones has increased, which allows a detailed overview to be obtained not only of the social bonds and habits of the individual, but also about their movement. The Petitioner considers the fact that the retention of traffic and location data also applies to persons with a duty of confidentiality, i.e. professional privilege (legal counsels, doctors, or advisers), to be no longer bearable. The blanket retention of sensitive data carries the risk of misuse: abroad, there have been cases of misuses of data regarding journalists (Poland) or the data have been used to identify participants in an anti-government demonstration (Belarus).

9. In addition, with regard to the various contested provisions, the Petitioner alleges that the definition of the purposes for which traffic and location data can be retained under national law is disproportionately broad and, as a result, violates Art. 15 (1) of Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended (hereinafter only as the "ePrivacy Directive"), as in this respect, the individual's privacy may be restricted solely for the purpose of safeguarding public security, national defence, and the prevention, investigation, detection and prosecution of criminal offences. The possibility of the use of traffic and

location data by the police in their search for a missing or wanted person cannot, by its very nature, justify exemptions to privacy protection, nor can the Czech National Bank's supervision of the capital market. The Petitioner is convinced that the authorisation under the provisions of Section 97 (3) (b) and (e) of Act No. 127/2005 Coll., on Electronic Communications and on Amendments to Certain Related Acts (Electronic Communications Act), as amended, (hereinafter only as the "ECA") in conjunction with Section 68 (2) and Section 71 (a) of Act No. 273/2008 Coll., on the Police of the Czech Republic (hereinafter only as the "Police Act" or "PolA") do not comply with the legitimate objectives defined exhaustively by the cited Directive.

10. In the narrower sense, in terms of the possibility to provide traffic and location data to law enforcement bodies pursuant to Section 97 (3) (a) of the ECA in conjunction with Section 88a of Act No. 141/1961 Coll., on Criminal Procedure (Criminal Procedure Code), as amended (hereinafter only as the "Criminal Procedure Code"), according to the Petitioner, the measure is not capable of meeting the legitimate objective of reducing crime and increasing its detection rate. According to the Petitioner, the available police crime statistics for the period of 2011-2013 imply that the possibility of using traffic and location data does not affect either the frequency or the detection rate of the crime – the same conclusions were drawn for serious crime, which should also be supported by foreign studies; law enforcement bodies are able to collect the necessary evidence using other methods. Furthermore, the Petitioner points out that monitoring of traffic and location data can be easily circumvented by means of various tools, e.g. by using an anonymous prepaid phone SIM card, which is particularly well-known to perpetrators of serious crime. The result is that the communication of the entire society which does not commit any crime is monitored in order to protect against offenders who know how to avoid surveillance technically – making the measure unsuitable in the proportionality test to meet a legitimate objective. In addition, it is obvious that the data in question are overused as they are not required only for the purposes of detecting particularly serious crime, but often serve as evidence in ordinary criminal proceedings.

11. In relation to Section 97 (3) (b) of the ECA, in conjunction with Section 68 (2) and Section 71 (a) of the Police Act, the contested legal regulation does not respect, according to the Petitioner, the conclusions of the Cassation Judgment file reference Pl. ÚS 24/10 (especially paragraph 36), according to which the provision of traffic and location data must be preceded by a decision of an independent court, which is not currently required by the Act. In some cases, the Police have access to traffic and location data without permission from the court, and are not obliged to use the data or subsequently inform their subject (as in the case of interception), so the person concerned will not even become aware of the interference with their constitutional rights.

III.

Standing to Sue and the Terms of the Proceedings

12. Under Section 64 (1) (b) of Act No. 182/1993 Coll., on the Constitutional Court, a group of at least 41 Deputies has the right to file a petition seeking the annulment of a statute or its individual provisions. Under Section 64 (2) (b) of Act No. 182/1993 Coll., on the Constitutional Court, as amended by Act No. 320/2002 Coll., a group of at least 25 Deputies may file a petition seeking the annulment of another enactment or its individual provisions. In the instant case, the petition was filed by a group of 58 Deputies and, in accordance with Section 64 (5) of Act No. 182/1993 Coll., on the Constitutional Court, as amended by Act No. 320/2002 Coll., the petition was complemented with the signature sheet in which each of them individually confirmed that they were joining the Petition. Therefore, the Petitioner has complied with the term of the standing to sue.

13. The petition complies with all the requirements prescribed by law and is admissible within the meaning of Section 66 of Act No. 182/1993 Coll., on the Constitutional Court, as amended by Act No. 48/2002 Coll.; at the same time, there is no reason to discontinue the proceedings under Section 67 of the same Act.

IV.

Course of the Proceedings before the Constitutional Court

14. Pursuant to Section 69 of the Act on the Constitutional Court, the Constitutional Court invited the Chamber of Deputies and the Senate of the Parliament and the Ministry of Industry and Trade as parties to the proceedings and the Government together with the Public Defender of Rights as secondary parties to the proceedings. Pursuant to Section 48 (2) of Act no. 182/1993 Coll., on the Constitutional Court, the Constitutional Court also invited the President of the Republic, the Ministry of Justice, the Supreme Public Prosecutor's Office, and the Office for Personal Data Protection to submit a statement on the petition.

15. The Public Defender of Rights notified the Constitutional Court that it would not intervene in the proceedings. The statement of the President of the Republic does not contain any substantial (new) facts, therefore the Constitutional Court does not consider it necessary to recapitulate in more detail.

a) Statement of the Chambers of the Parliament

16. In their observations, the Chamber of Deputies and the Senate merely described the course of the legislative process of adopting the contested regulation.

17. The Government bill of Act No. 273/2012 Coll., amending Act No. 127/2005 Coll., on Electronic Communications and on Amendments to Certain Related Acts (Electronic Communications Act), as amended, and certain other statutes containing the contested wording of Section 97 (3) and (4) of the ECA and Section 88a of the Criminal Procedure Code was sent to the Deputies as document No. 615 on 27 February 2012. The first reading of the bill took place on 14 March 2012, and subsequently the committees recommended adopting the bill. The bill passed the second reading on 14 June 2012. In the detailed debate, Deputy Jaroslav Krupka proposed a legislative and technical amendment consisting in renumbering the footnotes in association with the adoption of Act No. 142/2012 Coll., on Amendments to Certain Acts in Association with the Introduction of Basic Registers. The bill was adopted by the Chamber of Deputies in the wording of the amendment at the third reading on 20 June 2012. On 26 June 2012, the Chamber of Deputies referred the bill to the Senate, which adopted it as recommended by all the committees concerned in the wording adopted by the Chamber of Deputies as the Senate document No. 383 on 18 July 2012. At the Senate meeting, the Minister of the Interior emphasised that the legal regulation concerning the retention and use of traffic and location data was becoming significantly more stringent. The President of the Republic signed the Act and it was promulgated in the Collection of Laws on 22 August 2012.

18. The provisions of Section 88a of the Criminal Procedure Code were further amended by Act No. 455/2016 Coll., amending Act No. 40/2009 Coll., the Criminal Code, as amended, and other related statutes, the Government bill of which was sent to the Deputies as Parliamentary document No. 886 on 16 August 2016. The first reading of the bill took place on 16 September 2016 and 19 October 2016; the Chamber of Deputies adopted the bill in a special regime already at the first reading and subsequently referred it to the Senate on 4 November 2016. The Senate adopted the bill upon on the recommendation of the Committee on Legal and Constitutional Affairs in the wording adopted by the Chamber of Deputies as Senate document No. 348 on 30 November 2016. The President of the Republic signed the Act and it was promulgated in the Collection of Laws on 29 December 2016.

19. The Government bill on the Police, including the contested provisions of Section 68 (2) and Section 71 (a), was distributed to the Deputies as document No. 439 on 29 February 2008. The first reading of the bill took place on 25 March 2008 and was subsequently recommended by the committees to be adopted in the wording of the amendments proposed by them; the bill passed the second reading on 10 and 18 June 2008. Nine Deputies presented their amendments in a detailed debate. The bill was adopted in the wording of the amendments at the third reading on 25 June 2008. On 8 July 2008, the Chamber of Deputies referred the bill to the Senate, which approved it as recommended by all the committees concerned in the wording of the Chamber of Deputies as Senate document No. 301 on 17 July 2008. The President of the Republic signed the Act and on 11 August 2008, it was promulgated in the Collection of Laws.

b) Statement of the Ministry of Industry and Trade

20. The Ministry of Industry and Trade, which issued the contested Decree No. 357/2012 Coll. on the retention, transmission and destruction of traffic and location data (hereinafter only as the "Decree"), considers the legal regulation to be balanced and satisfactory. In support of its opinion, the Ministry refers to a communication of the Office for Personal Data Protection of 2012, which in the interdepartmental comment procedure identified the bill of the relevant amendment to the Electronic Communications Act as appropriate with regard to the scope and detail of the regulation and enshrining the right of an individual to be informed about processing their persona data. The Ministry of Industry and Trade also emphasises that operators, the Czech Telecommunication Office and the Office for Personal Data Protection were actively involved in drafting the Decree, drawn up in agreement with the Ministry of the Interior. The Decree was drafted as a compromise between the needs of entities concerned, technical capabilities of operators and privacy requirements.

c) Statement of the Government

21. In its observations, the Government (hereinafter only as the "Secondary Party") does not agree that the contested legal regulation does not respond to the relevant case law of the Court of Justice of the European Union and the Constitutional Court. According to the Government, the contested regulation responded adequately to all criticisms made by the Constitutional Court and cannot be reproached at all. In relation to the above-cited CJEU Judgments of Digital Rights Ireland Ltd and Tele2 Sverige AB, the Government points out that the Czech legal regulation was the subject of the review in neither of them, therefore the judgments could not entail a direct or indirect change for national legislation. The Government considers the Czech legal regulation to be strict and in compliance with the requirements of the Court of Justice of the European Union in comparison with other European countries.

22. Using practical examples, the Government demonstrates in what cases it would be impossible to detect crime without using legally retained traffic and location data. The Government argues that the Act on Electronic Communications not only provides for the required scope of retained data in terms of quantity and time interval beyond the data retained by obliged entities for their own needs (e.g. billing of services), but also a unified form of processing without which access to the requested data would become more difficult. The Government also considers as sufficient the requirements for securing the retained traffic and location data contained in Section 88 et seq. of the ECA.

23. With regard to Section 88a of the Criminal Procedure Code and the Petitioner's objection concerning the excessively broad definition of the concept of serious crime, the Government states that European Union law (hereinafter only as the "EU") does not provide a specific definition and it is up to the Member States to interpret the above concept. According to the Government, a number of restrictions and guarantees were added to the effective wording of Section 88a of the Criminal Procedure Code, already reflecting the requirements of both the Constitutional Court and the Court of Justice of the European Union and complying with the claims for protection of the fundamental rights concerned. The Government adds that the construction of guarantees and restrictions is almost identical to the requirements imposed on using interception and telecommunication traffic recording under Section 88 of the Criminal Procedure Code, except for the upper sentencing option and the subsequent exhaustive list of offences for which traffic and location data may be used. The indispensable added value of the retention of the data in question lies in detecting the information on telecommunication traffic, and thus, unlike Section 88 of the Criminal Procedure Code, it is directed to the past – while not concerning the content of the communication, which is another significant difference. In the view of the Government, the aforementioned provision would have withstood the proportionality test in all three steps.

24. Traffic and location data represent an important "electronic footprint", which plays an irreplaceable role and leads the Police to take further effective measures to detect the crime committed. In addition, according to the Government, obtaining traffic and location data protects the rights of third parties, as the Police eliminate possible suspects and assess that it is no longer necessary to interrogate a large number of persons, but only the relevant ones. The Government does not agree with the Petitioner's view that the perpetrators use mechanisms to ensure confidentiality of communication and that the contested instrument cannot therefore be regarded as effective, but rather consider it as an argument in favour of maintaining the obligation to retain traffic and location data and make them available to authorised bodies.

25. Regarding the alleged overuse of the contested institute, the Government emphasises the misinterpretation of statistics, which is caused by different methods of data processing by the Czech Telecommunication Office and the Police. The Government rejects the conclusion on the massive detection of traffic and location data by law enforcement bodies with reference to the charts contained in the statement.

26. The Government also considers the contested provisions of the Police Act to be satisfactory. Pursuant to Section 68 (2) of the aforementioned Act, the police are entitled to request the data in the case of searching for a missing or wanted person, which are terms defined by law; for these purposes, several terms and conditions must be cumulatively satisfied. The risk of abuse is minimal: the legal regulation is strictly set and is supplemented by equally strict internal acts. The absence of judicial review is justifiable by the need for a rapid response, as the health and life of the persons sought can be endangered. As for Section 71 (a) of the Police Act, concerning the prevention and detection of terrorist threats, the Government adds that it is a seldom-used provision according to statistics.

27. According to the Government, the Czech National Bank's authorisation to obtain traffic and location data for the prosecution of administrative offences in the capital market section is based on and consistent with the European legislation [Art. 69 (2) (r) of Directive 2014/65/EU of the European Parliament and of the Council of

15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU].

d) Statement of the Supreme Public Prosecutor's Office

28. The statement of the Supreme Public Prosecutor's Office focuses on the legal regulation concerning data retention in conjunction with Section 88a of the Criminal Procedure Code; it expresses the belief that, even if the Constitutional Court were to conclude on the unconstitutionality of Section 97 (3) and (4) of the ECA, Section 88a of the Criminal Procedure Code would be sustainable separately, as in the past. According to the Supreme Public Prosecutor's Office, the cited provision complies with the requirements of the Court of Justice of the European Union expressed in the Judgment of Tele2 Sverige AB, since serious crime is defined strictly enough here and other control mechanisms (in particular reasoned court orders) are also appropriate. The Supreme Public Prosecutor's Office opposes the Petitioner's assertion that the abundant use of traffic and location data by law enforcement bodies does not affect the rate of crime detection. According to the Supreme Public Prosecutor's Office, access to data is decisive for the direction and course (the speed and thus lower cost) of criminal proceedings; it is impossible to disregard the fact that, over time, crime is becoming more sophisticated, more frequently shifting to electronic communication platforms (including the Internet) and being committed using them.

29. In the light of the CJEU judgments, the Supreme Public Prosecutor's Office finds insufficient legal regulation contained in the Police Act, as it lacks the conditionality of police access with prior consent of an independent body deciding upon a reasoned application and the obligation to notify the person concerned of access to the retained data. However, the Supreme Public Prosecutor's Office considers the provisions of Section 68 (2) of the Police Act to be crucially important.

e) Statement of the Office for Personal Data Protection

30. In its observations, the Office for Personal Data Protection agreed with the petition seeking the annulment of the contested provisions; it believes that the criteria newly set out in the CJEU case law are not reflected in the Czech legal regulation. The Office highlights the contribution of the WP 29 expert group [Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established under Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (hereinafter only as the "WP 29")], which already in 2001, in the context of the fight against terrorism, highlighted the need for a balanced approach in terms of personal data protection as part of the individual's fundamental rights and freedoms. Even at that time, the WP 29 expressed concerns about the increasing tendency to classify the protection of personal data as an obstacle to the effective fight against terrorism and called for measures against terrorism not to lower the human rights standard.
31. In its observations, the Office for Personal Data Protection draws attention to the fact that the instant case must also be perceived in the light of the effective Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter only as the "GDPR", which seeks to strike a balance between the protection of fundamental rights and the development of communication technologies.

f) Petitioner's Response

32. The Constitutional Court sent the abovementioned observations to the Petitioner's representative to submit a reply. The Petitioner referred to the arguments put forward in the petition seeking the annulment of the legal regulations concerned and did not consider it necessary to respond further to the observations submitted.

g) Oral Hearing

33. The Constitutional Court listed a public oral hearing pursuant to Section 44 of the Act on the Constitutional Court, as in order to better clarify the technical context and details of the issue discussed, it was necessary to test the evidence by questioning informed persons from the professional public and practitioners under Section 49 (1) of the same Act. Mgr. Vanda Kellerová (representative of one of the largest operators on the market), doc. JUDr. Radim Polčák, Ph.D. (Head of the Institute of Law and Technology, Faculty of Law, Masaryk University), Mgr. Karel Bačkovský (Head of the Security and Legal Section, Security Policy Department of the Ministry of the Interior), JUDr. Tomáš Sokol (President of the Union of Defence Counsels of the Czech Republic, civil

association), Chief Public Prosecutor JUDr. Lenka Bradáčová and representatives of the relevant police departments (Col. Ing. Vladimír Šibor, Director of the Special Activities Unit of the Criminal Police and Investigation Service of the Police Presidium of the Czech Republic; Col. Ing. Bc. Josef Mareš, Deputy Head of General Crime Department of the Prague Police Directorate; and Col. Mgr. Bc. František Habada, Head of the Operational Department of the Police Presidium of the Czech Republic) were summoned to the oral hearing.

34. From the questioning of Mgr. Kellerová, the Constitutional Court found that law enforcement bodies in the past requested traffic and location data without specific data retention legislation, using other legal means (Section 8 of the Criminal Procedure Code). In the case of T-Mobile Czech Republic, a. s., data pursuant to Section 97 (3) of the ECA are kept separately, and access to them is subject to strict conditions; the costs incurred by the operator in relation to the fulfilment of this statutory obligation are borne by the State. The most frequently requested data are for the first three months from the moment of their origin. For its own needs (billing and complaints regarding the services), the operator keeps the traffic and location data (in a different extent than specified by the contested Decree, as it does not require all data for its needs) for a period of two months. For marketing purposes, data may be stored only with the consent of the customer (in the case of T-Mobile Czech Republic, a.s., this applies to approx. 70% of customers), the operator then keeps the data for six months. The annulment of the contested legal regulation would create a situation of considerable legal uncertainty for operators.

35. From the questioning of doc. Polčák, it was found that the contested legal regulation did not deviate from the European standard; it is possible to imagine that, for example, stricter requirements would be set for the security of retained data, or graduated access to them depending on the seriousness of the crime (rather than six months as a flat period for all legal purposes). The absence of data retention legislation in some States does not mean that the competent authorities do not use traffic and location data to investigate crime, but the information is obtained by other means.

36. The questioning of Mgr. Bačkovský established that the drafting of the bill of the contested regulation took place with the awareness of the Judgments of the Constitutional Court, file reference Pl. ÚS 24/10 and file reference Pl. ÚS 24/11; the establishment of a special office where data would be collected was also considered, yet the risk of their potential misuse in the case of central retention at one institution would be greater. According to him, the definition of crime pursuant to Section 88a of the Criminal Procedure Code is sufficiently strict; the use of traffic and location data in criminal proceedings is irreplaceable. Using Section 68 (2) of the Police Act serves to protect the life and health of missing persons; judicial review by nature does not make sense.

37. In his questioning, JUDr. Sokol stated that according to his practical experience, the record of traffic and location data is a marginal matter; it concerns a small number of cases, its informative value is rather supportive and circumstantial, not constituting inculpatory evidence.

38. From the questioning of JUDr. Bradáčová, the Constitutional Court found that due to social and technological developments, it is not possible to compare 2008 and 2019, as new and more sophisticated ("more modern") forms of crime arise each year. Considering the annual caseload of criminal matters, applications for the record of telecommunication traffic concern about 3% of cases. The record represents a milder measure and often serves as "starting" evidence, which in turn directs law enforcement bodies to use more invasive means (especially interceptions). Upon increasing the upper limit of the sentencing options in Section 88a of the Criminal Procedure Code, the mandatory data retention would not apply to a number of crimes which cannot be investigated without traffic and location data (spreading drug addiction, dangerous pursuit, dangerous threats, hate crime, scaremongering, or child pornography). It is a recent and modern footprint, an irreplaceable investigation method that has no adequate equivalent.

39. From the questioning of Col. Ing. Šibor, it was found out that all applications pursuant to Section 88a of the Criminal Procedure Code are processed and inquiries with operators carried out nationwide exclusively by the Special Activities Unit of the Criminal Police and Investigation Service of the Police Presidium of the Czech Republic (hereinafter only as the "Special Activities Unit"). Applications are authorised, inquiries are archived and may be retrospectively verified only through the Director of the Special Activities Unit. The record of traffic and location data is less invasive than interception, often preceding the interception permission. The report on telecommunications traffic (on "retained data") is important but not unique evidence, and must be supported by other evidence. The activities of the Special Activities Unit are regularly reviewed by the commission of the Chamber of Deputies (Standing Commission on Telecommunication Interception and Access, Spying and Interference to Electronic Communication) and the Office for Personal Data Protection.

40. The questioning of Col. Ing. Bc. Mareš implied that a record of traffic and location data is often used in investigating serious violent and property crime. While for violent crime, there is an advantage that the perpetrator must be physically present at the scene of the crime at some point, it does not have to be the case for property crime, and then the law enforcement bodies are often left with no more than electronic traces. The recording of telecommunications traffic also helps to exclude some individuals of interest (recidivists) from the list of suspects. In general, it is not possible to say whether a six-month period is necessary or redundant; it always depends on the circumstances of the particular case. At the time following the Constitutional Court's first intervention in the data retention area, 2-3 murders in his district could have remained unsolved due to the unavailability of traffic and location data.

41. From the questioning of Col. Mgr. Bc. Habada, in terms of the application of Section 68 (2) of the Police Act, the Constitutional Court found that its unit administers a central communication system into which missing persons are entered through fourteen regional offices handling emergency calls. Abuse does not occur, as requests for location data may be retrospectively verified. In addition, the informant is always personally confronted and "exhausted" by the police patrol, so they would change their mind about any possible abuse of the search. In approximately half of the cases, the missing person is found exactly where their electronic device was located. In this manner, for example, persons attempting suicide may be tracked in time, thus averting the consequences.

42. The following conclusion on the facts of the case was drawn from the evidence tested: the operators adapted to the contested legal regulation by creating new technical solutions, they did not incur any costs on their own and they do not incur them even in association with the processing of applications for access to traffic and location data, as these costs are borne by the State. The access to the data takes place exclusively through the Special Activities Unit; under the Police Act, it is possible to obtain only the location of the electronic device, rather than all traffic and location data as in the case of applications pursuant to Section 88a of the Criminal Procedure Code. The contested legal regulation does not deviate from the European standard. Just like technology, the form of committing crime has been developing, increasingly leaving only electronic traces of the perpetrators, so the investigation methods of previous years cannot be compared. To date, no system failure has been detected in relation to the retention of and access to traffic and location data.

V.

Review of the Procedure for Adopting the Contested Regulations

43. In accordance with Section 68 (2) of Act No. 182/1993 Coll., on the Constitutional Court, as amended by Act No. 48/2002 Coll., the Constitutional Court reviewed whether the contested provisions of the Electronic Communications Act, the Criminal Procedure Code and the Police Act were adopted and promulgated within the limits of the competence prescribed by the Constitution and in the prescribed manner. It concluded that there was nothing to be reproached to the legislature in this regard: the parties to the proceedings and the secondary party did not, after all, mention any deficiencies in the legislative process. For the sake of brevity, the Constitutional Court refers to a summary of the course of the legislative process in the statements of Parliament's chambers.

44. The Decree was issued by the Ministry of Industry and Trade. The competence of the ministries to issue regulations to implement the Act arises from Art. 79 (3) of the Constitution, yet it is subject in substance to the existence of an express statutory authorisation and its limits. In the instant case, the authorisation consists in the contested provision of Section 97 (4) of the ECA; the material condition for issuing a by-law has been complied with. The Decree was signed by the Minister of Industry and Trade and duly promulgated in the Collection of Laws with effect from 1 November 2012.

VI.

Substantive Review of the Petition

45. After reviewing the formal elements of the petition, the flawlessness of the process of adopting the contested regulations and the evidence tested, the Constitutional Court reviewed substantively the Petitioner's objections to the contested legal regulation and reached the following conclusions.

a) General Background

Right to Privacy, Information Self-Determination and Freedom of Communication

46. The retention of traffic and location data directly concerns the constitutionally guaranteed right to protection of private and family life within the meaning of Art. 10 (2) and (3) and Art. 13 of the Charter and Art. 8 of the Convention. Privacy constitutes one of the core elements of individual freedom, which is among the most important values of liberal democracy, and its protection is manifested in a number of different aspects, as evidenced by the comprehensive enshrining of this fundamental right in several different provisions of the Charter. The instant case concerns more specifically the right to information self-determination (Art. 10 (3) of the Charter) and freedom of communication (Art. 13 of the Charter). The right to information self-determination protects the individual from the unauthorised collection, disclosure or other misuse of personal data. Freedom of communication protects the confidentiality of letters and the confidentiality of communications, whether kept private or sent by post, by telephone, telegraph or another device or method.

47. The Constitutional Court has interpreted in detail the general principles concerning the right to privacy and the admissibility of restrictions to this right in favour of a constitutionally approved public interest already in the above-cited Judgment file reference Pl. ÚS 24/10, the reasoning behind which the Constitutional Court refers to especially in paragraphs 26 to 40. Briefly, the Constitutional Court explained in particular that, by its nature and importance, the right to information self-determination is among the fundamental human rights and freedoms, as together with personal freedom, freedom in the spatial dimension (home) and freedom of communication, it creates the individual's personality sphere, the individual integrity of which must be respected and consistently protected as the necessary condition for the dignified existence and development of human life overall. Respect and protection of this sphere are guaranteed by the constitutional order, as it is an expression of respect for human rights and freedoms (Art. 1 (1) of the Constitution).

48. The established case law of the Constitutional Court, particularly in relation to the issue of phone interception, unambiguously implies that the protection of the right to respect for private life within the meaning of Art. 10 (3) and Art. 13 of the Charter relates not only to the actual content of messages sent by telephone but also to the information about the called numbers, the date and time of the call, its duration, and in the case of mobile telephony, the call base stations [cf. for example the Judgment file reference II. ÚS 502/2000 of 22 January 2001 (N 11/21 SbNU 83), the Judgment file reference IV. ÚS 78/01 of 27 August 2001 (N 123/23 SbNU 197), the Judgment file reference I. ÚS 191/05 of 13 September 2006 (N 161/42 SbNU 327), or the Judgment file reference II. ÚS 789/06 of 27 September 2007 (N 150/46 SbNU 489)]. The traffic and location data constitute the specific information about the ongoing electronic communication.

49. Even though the content of the communication is not retained (unlike interception), the collected information may be used to compile a detailed record of an individual's movement and personal and communication profile (personal bonds, environment, social status, political orientation, health or sexual orientation). An individual means every user of a mobile phone and computer, i.e. almost every citizen of the Czech Republic. In addition, in the case of the Internet services, there is a very thin, sometimes barely discernible boundary between the traffic data and the content itself.

50. The so-called "metadata" of the communication (i.e. everything but the content) may be much more valuable and in fact "more dangerous" in terms of interfering with the privacy of the individual than knowing the content of the communication itself, as they are machine-readable and analysable; the future behaviour of the individual may be inferred from the results of such processing. Contrary to this, the content may in fact be "unsubstantial": if the communication participants do not wish it to be understandable, they communicate through hints or pre-agreed ciphers. The collection and retention of traffic and location data therefore also constitutes a significant interference with the right to private and family life and deserves a similar level of guarantees against abuse as the content of the communication itself in terms of the right to private and family life. It is therefore necessary to include in the scope of the protection of the fundamental right to respect for private life not only the protection of the actual content of messages sent by telephone communication or communication through public networks, but also traffic and location data about them (cf. the Judgment file reference Pl. ÚS) 24/10).

51. A fundamental right may be restricted only by law and only to the extent necessary in the conditions of a democratic rule of law state, while safeguarding the protection of the individual against acts of arbitrariness by the public authorities. In particular, restrictions on a fundamental right must comply with the requirements arising from the principle of the rule of law state and comply with the requirements arising from the proportionality test – in the case of conflicts of fundamental rights or freedoms with the public interest or other fundamental rights or freedoms, the purpose (objective) of the interference must be assessed in relation to the means used, whereas the principle of proportionality (in a broad sense) serves as the benchmark for assessment.

The legal regulation in question must be precise, unambiguous in its wording and sufficiently predictable to provide sufficient information to the potentially concerned individuals about the circumstances and conditions under which the state authority is entitled to interfere with their private life (Art. 2 (2) of the Charter) and where appropriate, they could adjust their behaviour so as not to conflict with a restrictive rule (Art. 2 (3) of the Charter). The powers conferred on the competent authorities and the modalities and rules for their implementation must also be strictly defined so as to provide individuals with protection against arbitrary interference.

52. The assessment of the admissibility of the particular interference under the proportionality principle (in a broader sense) involves three criteria. The first is the assessment of the eligibility (or appropriateness) of fulfilling the purpose – it is ascertained whether a particular measure is actually capable of achieving the intended objective of protecting another fundamental right or public good. Furthermore, the second step assesses the necessity: it is examined whether the one that was most considerate of the fundamental right was used in the selection of the means. Finally, the proportionality (in the narrower sense) is assessed, i.e. whether the harm to a fundamental right is not disproportionate in relation to the intended objective. Measures restricting fundamental human rights and freedoms must therefore not, in the case of a conflict of fundamental rights or freedoms with the public interest, outweigh, with their negative consequences, the positives represented by the public interest in the measures adopted [cf. the Judgment file reference Pl. ÚS 3/02 of 13 August 2002 (N 105/27 SbNU 177; 405/2002 Coll.)].

EU Law and the Court of Justice of the European Union

53. Pursuant to Art. 1 (2) of the Constitution, the Czech Republic shall observe its obligations under international law. EU law has been penetrating the Czech legal order through Article 10a of the Constitution, on the basis of which the Czech legislature has transferred part of its competences to the EU legislature. The relationship between the constitutional order of the Czech Republic and EU law, which also includes the CJEU case law, has undergone some development over time, on which the Constitutional Court has had other opportunities to comment in the past.

54. The Constitutional Court interpreted the content of Art. 1 (2) of the Constitution in relation to European Union law so that national legal regulations, including the Constitution, are to be interpreted in accordance with the principles of European integration and cooperation between EU bodies and Member State authorities. If there are several interpretations of the provisions of the constitutional order and only some of them lead to the achievement of the obligation assumed by the Czech Republic in association with its membership of the European Union, it is necessary to choose a euro-conforming interpretation supporting the implementation of the obligation, rather than the interpretation preventing the implementation [see the Judgment file reference Pl. ÚS 50/04 of 8 March 2006 (N 50/40 SbNU 443; 154/2006 Coll.) or the Judgment file reference Pl. ÚS 66/04 of 3 May 2006 (N 93/41 SbNU 195; 434/2006 Coll.)]. In other words, in the field falling within the scope of EU law, it interprets constitutional law with regard to the principles resulting from EU law [see also the Judgment file reference Pl. ÚS 36/05 of 16 January 2007 (N 8/44 SbNU 83; 57/2007 Coll.)]. All this applies while maintaining the limit, which is the substantive core of the constitutional order, i.e. the essential elements of a democratic rule of law state within the meaning of Art. 9 (2) of the Constitution [see the Judgment file reference Pl. ÚS 19/08 of 26 November 2008 (N 201/51 SbNU 445; 446/2008 Coll.)]. While EU law is not a reference criterion for assessing the constitutionality of a national legal regulation and a contradiction with a norm of EU law itself cannot lead to a derogation of a statute, it is necessary to take into account EU law and CJEU case law when interpreting the constitutional law.

55. The issue of data retention falls within the scope of EU law, as is apparent from the efforts of the European legislature to establish a single framework for national legislation. The Data Retention Directive, on the basis of which the contested legal regulation was adopted, was declared invalid by the Court of Justice of the European Union and the new European legal regulations have not yet been adopted. This has created legislative space freed by the invalidation of the Data Retention Directive, which Member States (including the Czech Republic) can fill up – since this is an area of competence shared by them with the EU (not an exclusive EU competence) – to the extent that the EU has not exercised or has ceased to exercise it effectively (Art. 2 (2) of the Treaty on the Functioning of the European Union); in filling the vacant legislative space, the legislature of a Member State takes due account of the substantial reasons of the CJEU judgment in which the EU legislation concerned was invalidated (here in particular the Judgment of Digital Rights Ireland Ltd).

b) Previous Case Law

56. The contested legal regulation of the Act on Electronic Communications and the Criminal Procedure Code was adopted in response to the aforementioned derogatory Judgments of the Constitutional Court file reference Pl. ÚS 24/10 and file reference Pl. ÚS 24/11. Subsequently, the Court of Justice of the European Union also delivered the Judgments in the matters of Digital Rights Ireland Ltd and Tele2 Sverige AB.

57. By means of the first of these Judgments file reference Pl. ÚS 24/10 of 22 March 2011, the Constitutional Court annulled the provisions of Section 97 (3) and (4) of the ECA, as amended, as well as Decree No. 485/2005 Coll., on the extent of traffic and location data, the time of retention thereof and the form and method of the transmission thereof to bodies authorised to use such data. The Constitutional Court applied the case law of the European Court of Human Rights (hereinafter only as the "ECtHR") on the use of interception (in particular the judgment in the case of Malone v UK, application No. 8691/79 of 2 August 1984) and reiterated its regulatory requirements allowing interference with the right to private life by public authorities. The European Court of Human Rights considers it necessary to define at a statutory level unambiguous rules governing the extent of the application of restrictive measures, setting the minimum requirements on the length and manner of retention of the information obtained, its use and third party access to it and establishing the procedures to protect the confidentiality of the information and its destruction; all so that individuals have sufficient guarantees of protection against abuse. Section 97 (3) of the ECA, as originally amended, did not clearly and precisely define the extent of the competent authorities, the purpose of providing the traffic and location data or the conditions for their use, even in association with the special regulations to which the contested norm referred. The Constitutional Court also criticised the absence of unambiguous and detailed rules containing minimum requirements for safeguarding the retained data (preventing third party access, establishing procedures to protect the confidentiality and integrity of the data, and procedures for their destruction) and guarantees against the risk of misuse.

58. Several months later, the Constitutional Court, following the Judgment file reference Pl. ÚS 24/10, also annulled by its Judgment file reference Pl. ÚS 24/11 of 20 December 2011 Section 88a of the Criminal Procedure Code due to its vagueness and uncertainty. In the proportionality test, the second criterion of necessity was not fulfilled, since the vague and broad formulation of the purpose ("detection of the facts relevant to criminal proceedings") made it possible to request and use data in virtually any context associated with any criminal proceedings. According to the Constitutional Court, this deficiency could not be overcome even by a constitutionally conforming interpretation. The Constitutional Court did not find a reason why the scope of the statutory guarantees for the use of instruments pursuant to Section 88 of the Criminal Procedure Code (interception – future telecommunication traffic including the content of communication) and Section 88a of the Criminal Procedure Code (traffic and location data – the past telecommunication traffic excluding the content of communication) should differ, since in both cases the intensity of interference with the right to private and family life is comparable. Beyond the requirements imposed on the legal regulation in question, in the Judgment file reference Pl. ÚS 24/10, the Constitutional Court added that effective protection against unlawful interference with the fundamental rights and freedoms of the persons concerned should be guaranteed through the obligation to additionally inform users of electronic communications services that their traffic and location data have been communicated to law enforcement bodies.

59. Later, the Court of Justice of the European Union, by means of the Judgment in the case of Digital Rights Ireland Ltd of 8 April 2014, declared the Data Retention Directive null and void for violation of Art. 7 (respect for private and family life) and Art. 8 (protection of personal data) of the EU Charter of Fundamental Rights. Although the Directive was capable of achieving the objective pursued (harmonisation of data retention in the field of combating serious crime), even such an objective alone could not justify the fact that measures concerning all electronic communications means and consisting in the retention of data of almost the entire European population were considered necessary. The Court of Justice of the European Union expressed a requirement for a targeted link between retained data and a threat to public security (data relating to a certain period of time, a certain geographical area or a circle of certain persons who may be involved in any manner in serious crime or in relation to person who, by means of retaining their data, could, for other reasons, contribute to the fight against serious crime).

60. Subsequently, by its Judgment in the case of the Tele2 Sverige AB of 21 December 2016, the Court of Justice of the European Union issued a preliminary ruling on the questions referred to by the United Kingdom and Sweden concerning the interpretation of Art. 15 (1) of the ePrivacy Directive in relation to the invalidation of the Data Retention Directive and the related consequences for the national legislation of the Member States. Pursuant to Art. 15 (1) of the ePrivacy Directive, Member States may adopt legislative measures restricting the scope of the protection of personal data within the meaning of the Directive where a restriction in a democratic society constitutes a necessary, adequate and proportionate measure to ensure national security (i.e. the security

of the State), defence, public security and the prevention, investigation, detection and prosecution of criminal offences or the prevention of unauthorised use of electronic communications systems. The Court of Justice of the European Union stated that the cited provision allowing Member States to derogate from the rule of the protection of personal data should be interpreted restrictively – it cannot be accepted that the exception becomes a rule, as is the case for large-scale and non-selective retention of substantial amounts of data. According to the CJEU, national legal regulation must effectively define the relationship between the data to be retained and the purpose pursued, i.e. it must allow for an effective definition of the scope of the measure (a circle of persons from the public the data of whom may at least have an indirect link with serious crime or contribute to combatting it and to preventing a serious threat to public security).

61. By another Judgment in the case C-207/16 of 2 October 2018 (Ministerio Fiscal), the CJEU partially relaxed the strict tone concerning the purpose of making available traffic and location data; it did not comment on the principle of data retention itself. As regards the question referred to by the Spanish court concerning the interpretation of the same provision as in the previous case (Art. 15 of the e-Privacy Directive), it found that the disclosure of information such as the name, surname and address of SIM card holders activated in a stolen mobile phone to public authorities for the purposes of their identification did not interfere with the fundamental rights of these holders, as enshrined in Art. 7 and 8 of the EU Charter of Fundamental Rights, in such a serious manner that their access to them should be limited, in the area of crime prevention, investigation, detection and prosecution, only to the fight against serious crime.

62. Recently, the European Court of Human Rights has also had the opportunity to recapitulate its case law on interception and to comment on data retention. In its Judgment of 13 September 2018, applications No. 58170/13, 62322/14 and 24960/15 (Big Brother Watch v the United Kingdom), in relation to providing communication data, it found a breach of not only Art. 8 of the Convention guaranteeing respect for private life, but also Art. 10 of the Convention, which guarantees freedom of expression. In particular, a breach of Art. 8 of the Convention consisted in the investigating authorities requesting data on several telephone numbers in order to disclose a journalist's information source (rather than an objective pursuing a defined public interest) and which was not subject to prior approval by a court or independent administrative authority. In these two aspects, according to the ECtHR conclusions, the procedure of the authorities concerned and the legislation in force in the United Kingdom were also incompatible with the requirements arising from the case law of the CJEU presented. In the absence of special legal regulation providing stricter protection for the use of traffic and location data in relation to the protection of the freedom of the press (activity of journalists), the Court also saw a violation of freedom of expression in the light of Art. 10 of the Convention.

c) Constitutional Law Review of the Contested Legal Regulation

63. The issues in the present case need to be divided into two levels which seem to be independent of one another but which, in reality, are connected vessels from the point of view of the constitutional law review.

64. At first, it is necessary to answer the question whether in the light of the fundamental rights set out above, it is admissible to generally, impersonally and preventively collect and retain data to the contested extent (Section 97 (3) and (4) of the ECA and Decree); it is thus necessary to review the statutory obligation to collect and retain the traffic and location data as such.

65. Secondly, in the event of a positive answer to the first question, it is necessary to address the question of appropriately defining the circle of authorities authorised to access the data collected in relation to setting legitimate objectives to be satisfied by the use of traffic and location data, including the determination of the statutory terms and guarantees for minimising the interference with the fundamental rights of individuals [Section 97 (3) of the ECA, Section 88a of the Criminal Procedure Code, and Section 68 (2) and Section 71 (a) of the Police Act].

66. The Constitutional Court took into account the arguments of the parties, assessed the evidence, then carried out the proportionality test, and concluded that the current data retention regulation complies with the requirements laid down by the quoted earlier case law of the Constitutional Court and may be applied in a constitutionally conforming manner, i.e. protecting the rights of individuals guaranteed by Art. 10 and 13 of the Charter to the maximum possible extent. The application has therefore been dismissed for the following reasons.

Contested Legal Regulation

67. The provisions of Section 97 (3) and (4) of the ECA, as amended before the amendment adopted in Act No. 287/2018 Coll., read as follows:

Interception and Recording Messages
Section 97

…
(3) A legal entity or natural person operating a public communication network or providing a publicly available electronic communications service shall retain, for a period of 6 months, traffic and location data created or processed in the provision of its public communication networks and in the provision of its publicly available electronic communications services. A legal entity or natural person providing a public communications network or a publicly available electronic communications service shall retain traffic and location data related to unsuccessful call attempts only if such data are created or processed and at the same time retained or recorded.

At the same time, this legal entity or natural person shall ensure that when fulfilling the obligation under the first and second sentence, the content of the messages is not retained and transmitted as retained in this manner. The legal entity or natural person retaining traffic and location data shall provide them upon request without undue delay:

a) To law enforcement bodies for the purposes and under the conditions stipulated by a special legal regulation;
b) To the Police of the Czech Republic for the purpose of an initiated search for a specific wanted or missing person, identification of a person of unknown identity or identity of a found corpse, prevention or detection of specific threats in the area of terrorism or screening of a protected person, and under the conditions stipulated by a special legal regulation;
c) To the Security Information Service for the purposes and under the conditions stipulated by a special legal regulation;
d) To the Military Intelligence for the purposes and under the conditions stipulated by a special legal regulation;
e) To the Czech National Bank for the purposes and under the conditions stipulated by a special legal regulation.

Upon the expiry of the period referred to in the first sentence, the legal entity or natural person retaining traffic and location data shall destroy them unless provided to the authorities authorised to use them pursuant to a special legal regulation or unless this Act provides otherwise (Section 90).

(4) Traffic and location data pursuant to paragraph 3 means, in particular, data leading to tracing and identification of the source and addressee of the communication, as well as data leading to determining the date, time, method and duration of the communication. The extent of traffic and location data stored pursuant to paragraph 3, the form and manner of their transmission to the authorities authorized to use them pursuant to a special legal regulation and the method of their destruction shall be laid down in an implementing legal regulation.

…

68. Due to its extent, the Constitutional Court does not consider it necessary to quote the wording of the Decree; for the purposes of the reasoning behind the judgment, it is sufficient to briefly recapitulate its wording, which specifies the type of retained data. Pursuant to Section 2 of the Decree, these are, in particular, telephone numbers of communication participants, date and time of commencement of communication (sending the message), length of communication, for mobile telephones also the IMSI identifier (the international mobile subscriber identifier assigned by the operator), and the identifier of the mobile device of the communication participants. In the case of Internet services, the retained data include in particular the type of connection, user identification, date and time of the Internet connection, access point identification, IP address and, in the case of electronic communication services, information about the connection to an electronic mail box and sending and receiving mail including sender and recipient addresses. Furthermore, the Decree regulates the details of the process of providing retained data to competent authorities and their destruction upon the expiry of the statutory period.

69. The provisions of Section 88a of the Criminal Procedure Code read as follows:

Section 88a

(1) If it is necessary for the purposes of criminal proceedings conducted for an intentional criminal offence, for which the law prescribes a sentence of imprisonment with an upper limit of at least three years, for criminal offences of breach of secrecy of correspondence (Section 182 of the Criminal Code), fraud (Section 209 of the Criminal Code), unauthorised access to computer systems and information media (Section 230 of the Criminal Code), obtaining and possession of access device and computer system passwords and other such data (Section 231 of the Criminal Code), dangerous threatening (Section 353 of the Criminal Code), dangerous pursuing (Section 354 of the Criminal Code), spreading of alarming news (Section 357 of the Criminal Code), incitement to criminal offence (Section 364 of the Criminal Code), approval of criminal offence (Section 365 of the Criminal Code) or for an intentional criminal offence, prosecution of which is stipulated by an international treaty binding the Czech Republic, to ascertain data on telecommunication traffic that are subject to the telecommunication secrecy or to which applies protection of personal and mediated data and if the followed purpose cannot be achieved otherwise or achieving it would be substantially more difficult, the presiding judge shall order the data to be submitted to the court in trial proceedings, and in pre-trial proceedings the judge shall order it to be submitted to the public prosecutor or to the Police authority upon a motion of the public prosecutor. The order for ascertaining data on telecommunication traffic must be issued in writing and must be reasoned, including a specific reference to a promulgated international treaty if the criminal proceedings is being conducted for a criminal offence, prosecution of which is stipulated by this international treaty. If the request concerns a specific user, the order must include his identity, if it is known.

(2) The public prosecutor or the Police authority, by whose decision the case was finally and effectively terminated and in trial proceedings, the presiding judge of the panel of the court of the first instance shall inform the user referred to in sub-section (1), if he is known, after the final and effective termination of the case, about the ordered ascertaining of data on telecommunication traffic. The information contains identification of the court that issued the order for ascertaining of data on telecommunication traffic and data on the period concerned by this order. The information shall also contain an instruction on the right to file a petition for a review of the legality of the order for ascertaining of data on telecommunication traffic with the Supreme Court within six months from the day of service of this information. The information shall be submitted by the presiding judge of the panel of the court of the first instance without undue delay after the final and effective termination of the case. The public prosecutor, by whose decision the case was finally end effectively terminated shall submit the information without undue delay after the expiration of the time limit for his decision being reviewed by the Supreme Public Prosecutor according to Section 174a and the Police authority, by whose decision the case was finally and effectively terminated, shall submit the information without undue delay after the expiration of the time limit for his decision being reviewed by the public prosecutor according to Section 174 (2) (e).

(3) The information according to sub-section (2) shall not be submitted by the presiding judge, the public prosecutor or the Police authority in the proceedings on a felony for which the law stipulates a sentence of imprisonment with an upper limit of at least eight years, committed by an organised criminal group, in proceedings on a criminal offence committed in favour of an organised criminal group, in proceedings on a criminal offence of participation in an organised criminal group (Section 361 of the Criminal Code), in proceedings on the criminal offence of participation in a terrorist group (Section 312a of the Criminal Code), or if several persons took part in commission of the criminal offence and in relation to at least one of them, the criminal proceedings was not finally and effectively terminated, or if criminal proceedings is being conducted against the person to whom the information is to be conveyed, or if providing such information could compromise the purpose of this or another criminal proceedings, or if it could lead to the security of State, or the life, health, rights or freedoms of persons being endangered.

(4) The order according to sub-section (1) is not necessary, if the user of the telecommunication device to which the data on the completed telecommunication are to be related grants his consent to submitting the data.

70. The provisions of 68 (2) and Section 71 (a) of the Police Act read as follows:

Section 68

Searching for persons and things

(2) For the purpose of an initiated search for a specific wanted or missing person and for the purpose of the identification of a person of unknown identity or the identity of a found corpse, the Police may request the provision of traffic and location data from a legal entity or natural person providing a public communication network or providing a publicly accessible electronic communication service in a manner allowing remote and

uninterrupted access, unless any other legal regulation provides otherwise. The information shall be provided in the form and to the extent stipulated by another legal regulation.

…

Section 71

The Police unit in charge of combating terrorism may, for the purpose of preventing and detecting specific threats in the area of terrorism and to the extent necessary request:

a) A legal entity or a natural person providing a public communication network or providing a publicly accessible electronic communication service to provide traffic and location data in a manner allowing remote and uninterrupted access, unless any other legal regulation provides otherwise; the information shall be provided in the form and to the extent stipulated by another legal regulation;

…

Data Retention Principle

71. First of all, according to the Constitutional Court, it is necessary to address the question of the admissibility of the statutory principle of blanket retention of traffic and location data by private entities as such in terms of limiting the fundamental rights concerned. The Charter permits limitations of personal integrity and privacy by public authorities only in exceptional cases, i.e. if necessary in a democratic society, unless the objective pursued by the public interest can be achieved otherwise and if it is acceptable from the point of the statutory existence and observance of effective and specific guarantees against arbitrariness.

72. The currently contested provisions of Section 97 (3) and (4) of the ECA and Section 88a of the Criminal Procedure Code were adopted by Act No. 273/2012 Coll., taking effect on 1 October 2012, in response to the Judgment file reference Pl. ÚS 24/10. In its cited Judgment, which annulled the earlier wording of Section 97 (3) and (4) of the ECA, the Constitutional Court concluded that blanket and preventive collection and retention of data constituted an interference with the right to privacy and information self-determination so intense that the most stringent standards possible need to be applied to the compliance with the above requirements concerning the admissibility of the interference, and the previous legal regulation contained in the Electronic Communications Act failed to stand the test in this respect according to the Constitutional Court. In its Judgment cited above, the Constitutional Court, as obiter dictum, expressed its doubts as to the necessity and proportionality of the tool of blanket and preventive metadata collection of all electronic communications in terms of the intensity of interference in the private sphere of a significant number of individuals, as well as the fact that the sensitive data are concentrated in the hands of private entities – operators (i.e. providers of Internet services and telephone and mobile communications).

73. The legislature responded to the Constitutional Court's criticisms by reducing the retention period for traffic and location data to six months, explicitly listing the entities authorised to request retained data, including the purposes for which authorised entities may request the data, complementing the legal definition of traffic and location data, and again referring in detail to the implementing regulation (the contested Decree).

74. In the meantime, the Data Retention Directive, on the basis of which the principle of data retention was introduced into the Czech legal system (see paragraph 59), was annulled by the CJEU Judgment in the case of Digital Rights Ireland. In response to this judgment, the Member States referred the questions to the Court of Justice of the European Union for a preliminary ruling concerning the compatibility of national regulations on the retention and management of traffic and location data with the ePrivacy Directive, of which the Judgment in the case of Tele 2 Sverige AB plays an essential role (see paragraph 60). According to this case law, the Court of Justice of the European Union found the principle of a general and blanket collection of all data on all electronic communications contrary to Art. 15 (1) of the ePrivacy Directive, or possibly Art. 7 and 8 of the Charter of Fundamental Rights of the European Union, guaranteeing the protection of privacy and personal data. However, there is no political consensus at the European level concerning the form of a unified regulation of data retention, as evidenced by the fact that, since the invalidation of the Data Retention Directive by the Judgment in the case of Digital Rights Ireland, no new legislation has been drafted to replace the specific directive. At the level of national legislation, different approaches by legislatures can therefore be encountered.

75. In order to offer an idea of possible alternatives, the Constitutional Court provides examples from the geographically and historically closest, i.e. neighbouring, countries. In Germany, after the cassation intervention of the Federal Constitutional Court [the Judgment of 2 March 2010, file reference 1 BvR 256/08 (BVerfGE 125, 260-385)], the new and largely restrictive data retention legislation was adopted. The newly defined traffic data categories may be retained only for a period of ten weeks, and location data only for four weeks. Furthermore, the categories of data that must not be retained at all are defined (in addition to the content of the communication, e.g. data on visited websites and electronic mail services); in addition, a "data freeze" mechanism (the collection of future telecommunications traffic data of a specific suspect at the initiative of a law enforcement body) was introduced to complement it. In Slovakia, after the intervention of the local Constitutional Court (the Judgment of 29 April 2015, file reference PL. ÚS 10/2014), the legislature abandoned the principle of blanket data retention and instead introduced the "data freeze" mechanism, which is similar to interception in terms of the time perspective, as it does not make data available backwards in the past. In Austria, following the intervention of the Constitutional Court (see the Judgment of 27 June 2014, file reference G 47/2012 and others), no new legal regulation has yet been adopted, as there has been no political consensus on this issue. It is only in Poland where at present it is possible to find a more liberal legal regulation in terms of the protection of the individual's privacy and more benevolent to the protection of the security of the State and its citizens; the time limit for metadata retention is not stipulated by law and no prior judicial consent is required; courts are only sent statistics on the data obtained at half-year intervals. This regulation is currently (and for the second time) under review by the Polish Constitutional Tribunal following the Ombudsman's petition.

76. The Constitutional Court is now returning to assessing the admissibility of the data retention principle as such, and states that if it was reluctant to explicitly express on the disproportionateness of the principle in 2011, it is not possible to reach such a conclusion today. Since the last decision-making on the matter, there have been substantial information technology developments, individuals have been using electronic communications services more and more frequently, telecommunication traffic data are generated by them as a result of their activity, they exist and are retained by operators (private entities with which customers have concluded private law contracts) for a certain period of time (the provision of the services, their subsequent billing, complaints, etc.); moreover, most customers grant their consent to the processing of their data beyond what is necessary to provide the requested service (for marketing purposes). It is thus an undeniable fact that data on an individual's electronic communication will always be collected in a certain form, even without any data retention regulation (i.e. without a legal obligation to "retain" them), otherwise electronic communication would not be possible at all.

77. In other words, traffic and location data on electronic communications are not retained solely because of a statutory obligation, but are and will be retained for the purposes of providing these services, their billing and settlement of any potential complaints even without a statutory obligation (in a more or less identical extent and for a more or less identical period of time). As implied, for example, from the testimony of doc. Polčák, the absence of the legislatively introduced principle of data retention in a specific Member State does not mean that public authorities do not work with traffic and location data; they only obtain them in different manners. It is thus impossible to guarantee that these alternative methods are less invasive in terms of the interference with the right to privacy than the procedure under the legal regulation using the data retention principle.

78. Therefore, the Constitutional Court logically considered which of the options constituted a "lesser evil" and concluded that in terms of transparency of the procedure of public authorities, as well as supervising the interferences with the individual's privacy, it is better to provide an unambiguously, precisely and sufficiently strictly defined legal framework of the data retention principle (see below), rather than a "'legislative shadow" which would otherwise be used by the operators when retaining traffic and location data and public authorities (particularly law enforcement bodies) in an attempt to gain access to them. It is a misconception that abandoning the data retention principle eliminates the risk of misuse of the created data.

79. It may appear that, by means of its current approach, the Constitutional Court, as the guardian of constitutionality, paradoxically provides the individual's privacy with a lower level of protection than the Court of Justice of the European Union, the primary mission of which does not consist in the protection of fundamental rights and which, with reference to privacy, takes a (generally) negative view of the principle of data retention a priori. However, the opposite is true – in particular, with reference to the requirement of predictability, unambiguousness and strictness of the legal regulation interfering with the right to privacy. With its approach, the Constitutional Court protects the individual's privacy more than if its intervention provided room to seek other, alternative and less transparent manners to access electronic communication metadata. Indeed, the rejection of the data retention principle would not result in a situation in which traffic and location data would not be generated and retained and used (at least by law enforcement bodies); on the contrary, it would result in

the loss of public service limits and supervision over the extent of the retention of traffic and location data, the manner in which they are secured and their disclosure. Responsibility for handling traffic and location data by public authorities would then de facto be transferred from the State to operators (private entities), which would be an unacceptable situation in the rule of law state.

80. The Constitutional Court cannot disregard the social and technological developments outlined above since its last decision in the matter. Interpersonal communication has been increasingly shifting its focus to the environment of telecommunication and electronic services. In the present situation, it would therefore be unwise to prevent the State, as the bearer of a number of tasks, to fulfil its specific public interests (in particular, the State security, the protection of the health and property of the population) to have access to data that can be a valuable source of important information under appropriate terms and conditions. The Constitutional Court therefore does not condemn the principle of data retention as such (as in the underlying reasons for the Judgment file reference Pl. ÚS 24/10); after all, the legislature is obliged to impose an obligation on operators to collect real-time traffic data on the basis of an obligation under the Convention on Cybercrime, promulgated under No. 104/2013 Coll. of International Treaties.

81. The Petitioner opposes the very existence of the data retention principle, inter alia, by asserting that professional privilege has been jeopardised (attorneys, social workers, or telephone counselling centre workers). This claim could be supported following the assumption that the purpose for which the traffic and location data can be requested was not sufficiently defined and the conditions of access to it were not properly set, including the guarantees of the persons concerned against the arbitrariness of the competent authorities (see below). However, it is impossible to see any undue interference with the privacy of persons bound by confidentiality obligations in the secure retention of electronic communication data without linking it to a competent authority. In the case of a request for access to confidentiality data of protected electronic communication – and not only but in principle always – it is up to the applying authorities (especially the courts) to decide, according to the specific circumstances of the case, whether the interest in achieving the objective pursued by using traffic and location data prevails (for the purposes of fulfilling a specific public interest), and it is therefore reasonable to disclose the data or whether the interest in protecting the privacy and confidentiality of the circumstances of the communication undertaken prevails, thus rejecting access to traffic and location data.

82. With respect to the above, the Constitutional Court did not find reasons for allowing the petition solely on the ground that the blanket and impersonalised collection of traffic and location data on the communication was a priori disproportionate in relation to the privacy protection. Thus, if, in the subsequent proportionality test, the conditions for retaining and accessing traffic and location data are found to be sufficiently stringent and counterbalancing limitations of the right to private and family life under Art. 10 (2) and (3) are met in conjunction with Article 13 of the Charter, the Constitutional Court has not found space to allow the petition.

Conditions for Retaining Traffic and Location Data

Purpose of Retention and Disclosure of Traffic and Location Data

83. In the first step of the proportionality test, it is necessary to examine whether the legal regulation pursues a legitimate aim and whether the resulting interference with the fundamental right caused by the regulation is capable of attaining the objective pursued. The purpose of the data retention regulation cannot be inferred from the very wording of Section 97 (3) of the ECA, but only in combination with Section 88a (1) of the Criminal Procedure Code and other regulations referred to in determining the competences of individual authorities. Thus, in order to define the objective of the contested legal regulation, it is also necessary to take into account who has legitimate access to the retained data, since this fact is linked to the purpose for which the competent authorities may request access.

84. According to the statement of reasons, the purpose of collecting traffic and location data consists in subsequently using them to detect selected crime (Section 88a (1) of the Criminal Procedure Code), searching for missing or lost persons (Section 68 (2) of the Police Act); fighting against terrorism [Section 71 (a) of the Police Act], the activity of intelligence services (acquisition, collection and evaluation of information important for the protection of the constitutional system, important economic interests, security and defence of the Czech Republic – see Section 2 of Act No. 153/1994 Coll., on Intelligence Services of the Czech Republic) and in the supervision of the capital market (Section 8 of Act No. 15/1998 Coll., on Supervision in the Capital Market Area and on Amendments to Other Acts, as amended).

85. All the above objectives pursue a strong public interest (protection of the security and health of the population and economic interests of the State) and as such may be described as legitimate. Undoubtedly, the information obtained by the competent authorities from the requested traffic and location data is capable of moving them forward in their activities and directing them one step closer to the fulfilment of the above purpose, whether it is (to put it in a simplified and metaphorical manner) detecting crime, finding a lost senior citizen, or averting a terrorist threat.

86. Furthermore, it is necessary to address the question of the need, i.e. the need to limit the right to private and family life in relation to the objective pursued. The Constitutional Court examined whether there were milder and less invasive means that are also capable of achieving the defined objective and concluded that the use of traffic and location data did not have an actual equivalent: there are no means with which to compare the instrument under examination. Although the Constitutional Court compares, at several points of this and earlier judgments, the use of traffic and location data in criminal proceedings in terms of the intensity of interference with the privacy of individuals with interception, they are not identical. While by means of ordering the interception, the suspect may be monitored in the future, traffic and location data allow the competent authorities to obtain information about an act that has already happened: the competent authorities will not be able to access such information otherwise. What would be equally unreasonable is a comparison to the tracking of persons and things under Section 158d of the Criminal Procedure Code, because even in this case, the competent authority obtains not more than the information on the movement and communication of the person in real time, but not in the past. For these reasons, the above-mentioned so-called "data freeze" mechanism (paragraph 75) cannot be deemed as an adequate and less invasive replacement either, even though some countries (e.g. Slovakia) have used it to replace the data retention principle or substantially restricted it, while complementing it with the data freeze mechanism (e.g. Germany) – even here, the competent authority obtains access only to data following the issuing of the relevant order, rather than past data. As there is not a means of obtaining the same information as may be drawn from traffic and location data, it is not possible to terminate at the second step of the proportionality test, since the contested legislation has also complied with it.

87. The Constitutional Court has therefore shifted the focus of its attention to the final step of the proportionality test, which consists in the measurement – the proportionality of the limitation of the fundamental right to private and family life in favour of the pursuit of public interest objectives in the narrower sense. It is necessary to answer whether the public interest concerned is sufficiently important to justify the extent of the limitation of the privacy by monitoring the electronic communication of almost the entire Czech population for a period of six months "in stock" by commercial entities, whether the contested legal regulation could limit the interference with the right to private and family life more, i.e. whether the statutory setting of the conditions is sufficient and provides sufficient safeguards against the misuse of this important instrument to counterbalance the limitations.

88. The Constitutional Court focused on particular issues which, taken together, affect the assessment of the proportionality of the contested regulation in the narrower sense. In particular, it is necessary to address the statutory period during which mandatory data are retained. It is also necessary to resolve whether the circle of authorities competent to access the retained data (depending on the objective and the conditions under which they can obtain the data) is not set too broadly. And finally, it is essential that the individual be provided with sufficient means of protection against the misuse of retained data (both in terms of safeguarding and unauthorised access to the retained data, as well as the individual's procedural defence means in the case of suspicion that their data have actually been misused).

The Period of Retention of Traffic and Location Data

89. With regard to the six-month period during which the traffic and location data are retained pursuant to Section 97 (3) of the ECA, the Constitutional Court proceeded from the fact that its length represents the most moderate option out of the possibilities set forth by the Data Retention Directive, which was still in force at the time of adopting the contested legal regulation. However, it is necessary to ask whether the six-month period is appropriate in today's conditions. The testimony of an informed person from among the operators revealed that the maximum period for which the operator needs to retain the metadata in question for its own needs does not exceed two months. At the same time, however, the operator keeps the selected data (in the extent not identical to the extent prescribed by law) for marketing purposes for a period of six months based on the consent granted by the customer. In the specific consent regime, for example, T-Mobile Czech Republic, a.s. currently retains the data of approximately 70 % of customers.

90. At this point, particularly in association with criminal investigations, it is necessary to distinguish that data are required in principle in two manners. Either the competent authority has data available in relation to a

specific user (their mobile number, fixed line, IP address, IMEI, etc.), in which case it is interested in listing voice or data services, i.e. contacts, activity, or movement of the user (their phone, computer, etc.), or the authority does not know this data but has information on where the user of interest was located or where the crime was committed. In the latter case, the competent authority is particularly interested in data from individual BTSs (cells), determining, for example, which mobile phones were currently connected to the given cell.

91. Based on the testimony of Col. Ing. Šibor at the public oral hearing, the Constitutional Court found that most inquiries concern precisely BTS stations' statements which are not older than a few days; older inquiries about this type of statements is not even technically possible.. Furthermore, the testimony of Col. Ing. Bc. Mareš implied that in the case of records of voice or data services of a particular user, the law enforcement body typically uses the maximum possible extent of six months. Information collected from a single telecommunications traffic statement is often packed with additional insights allowing, for example, networks of offenders or organised groups to be detected. Therefore, regardless of the specific facts of the case under examination, it is not possible to reach a generalised conclusion concerning the extent to which the information is necessary or useful to the law enforcement bodies covering the entire period of six months in order to fulfil the objective pursued; it may only be stated that the competent authorities use the maximum time allowed by law if they are aware of the identification data of a specific user. However, since the frequency of inquiries for base stations is much higher than statements of particular subscriber numbers or mobile devices, it may be concluded, in terms of the total number of all inquiries, that most of the required data are not older than three months (see also the testimony of Mgr. Kellerová).

92. Although traffic and location data older than three months are used only to a limited extent, in the Constitutional Court's view, it is not possible to conclude that older metadata in specific cases (especially in the application of Section 88a of the Criminal Procedure Code) would not be necessary and useful and therefore disproportionate in relation to the objective pursued. The legislature in response to the Judgment file reference Pl. ÚS 24/10 opted for the six-month "retention period" as the shortest possible according to the then valid Data Retention Directive. If the Constitutional Court did not conclude that the principle of data retention was unconstitutional on its own and unless it was established in the proceedings before the Constitutional Court that the retained data were not used or were overused, i.e. the right to private and family life was not protected by the competent authorities, it is not possible to conclude on the inadequacy of the retention period thus determined. There is never a single right solution to regulate a certain area of social relations. Certainly, from the point of view of minimising the interference with the privacy of telecommunication traffic subscribers, a stricter regulation can be imagined, for example (as Dr. Polčák testified) distinguishing and graduating access to traffic and location data according to the objective the fulfilment of which the competent authority pursues and the consequent actual needs for obtaining the data for a certain period (cf. the legal regulation adopted in Belgium or Germany). However, it is up to the legislature to decide what solution it will opt for when regulating the retention period and access to data. Nevertheless, if it protects the privacy of an individual so that the legal regulation of data retention corresponds to the actual need for the use of traffic and location data, it is not for the Constitutional Court to intervene in its legislative power.

Security of the Retained Traffic and Location Data

93. In addition, the legal regulation protecting the right to private and family life to the maximum possible extent also needs to comply with the requirement of determining unambiguous and detailed rules when securing the retained data and guarantees against their misuse (unauthorised and arbitrary access). Especially in the case of data retention, the quantity of data on all users of electronic communications is concentrated in private entities and therefore the legislature must be twice as strict. It needs to be unambiguously determined that traffic and location data must be retained securely and may not serve the marketing purposes of obliged entities without the express consent of the clients within the meaning of the applicable regulation of the personal data protection. At the same time, however, the dynamic development of the information technology sector has meant that the legislature is always a few steps behind; therefore, it may even be advantageous if data security at the statutory level is formulated more generally and if the technical details are left to the implementing regulation, which may respond more quickly and flexibly to changes in practice.

94. The securing of retained data is contained in Section 87 et seq. of the ECA (which represents the implementation of the e-Privacy Directive) together with the general data protection regulations – GDPR (except Art. 95 defining the relationship between the Regulation and the e-Privacy Directive) and transposing Act No. 110/2019 Coll., on Processing Personal Data. Although the specific passage of the Electronic Communications Act regulating data security has not been contested, the Constitutional Court cannot resign from the assessment of this aspect, as the method of securing the retained (provided) traffic and location is closely related to the

review of the adequacy of the data retention principle, i.e. with the constitutionality of the contested provisions of Section 97 (3) and (4) of the ECA.

95. In general, it may be stated that the level of security of traffic and location data is not lower than the level of security of other data processed under the Electronic Communications Act – see Section 88a of the ECA (amended in the same manner as the contested provisions by Act No. 273/2012 Coll. in response to the Judgment file No. Pl. ÚS 24/10), as a result of which the traffic and location data are explicitly assigned to the level of personal data from the security perspective. The Act imposes an obligation on operators to secure retained traffic and location data and also regulates the mechanism for reviewing and checking the compliance with specified obligations by independent institutions. Specifically, the operator, as a data processor, is obliged: to ensure the technical and organisational security of the service provided and to prepare internal technical and organisational regulations to provide data protection and communications confidentiality (including the confidentiality of traffic and location data related to the communication) [Section 88 (1) (b) in conjunction with Section 89 of the ECA]; to inform subscribers concerned about the risk of breach of security of services, protection of personal data and confidentiality of communications [Section 88 (1) (c) of the ECA]; to establish internal procedures for processing users' requests for access to their personal data [§ 88 (1) (d) of the ECA]; to notify the Office for Personal Data Protection of cases of breaches of personal data protection, including the solution, and to keep records of such cases (Section 88 (4) to (7) of the ECA); not to process traffic and location data for marketing purposes without the consent of the person concerned (Section 90 (6) of the TEC); to limit to the necessary minimum both the scope of the retained data and the range of persons (authorised employees) authorised to access and further process the retained data (Section 90 (9) and Section 91 (4) of the ECA); to maintain the confidentiality of requesting and providing data pursuant to Section 97 (3) of the ECA (Section 97 (8) of the ECA); to keep records of cases of access to traffic and location data and to regularly "report" it to the Czech Telecommunication Office (Section 97 (10) and (11) of the ECA).

96. A breach of any of the above obligations by the operator constitutes an administrative offence [see particularly Section 118 (12) (a) and (d) and (14) (b) to (h), (k), (z), (aa), and (ae) and (15) of the ECA], the commitment of which may be, in some cases, subject to a penalty of up to CZK 50,000,000 or up to 10% of the net turnover [Section 118 (23) (c) of the ECA], which is the strictest category of sanctions for administrative offences under the Electronic Communications Act. The Czech Telecommunication Office, which has a number of other supervisory powers in relation to the operators, is competent to deal with administrative offences under this Act. In the area of data retention, compliance with the general regulations concerning personal data protection during processing by operators is also subject to supervision by the Office for Personal Data Protection (Section 87 (3), Section 88 (4) to (7) of the ECA).

97. As it is obvious from the above list, according to the Constitutional Court, there are a number of safeguards against misuse of retained data in the legal order; the level of the security of the data collected is sufficient; thus, the above-mentioned aspect of the examined issue does not constitute unconstitutional inadequacy of the contested legal regulation of data retention (in particular § 97 (3) and (4) of the ECA and the Decree). In this respect, what also remains irrelevant are the conditions of access of the competent authorities to the requested data (see below) and the fact that the competent authorities do not have any database of data in which they could arbitrarily search.

Conditions of Access to Traffic and Location Data

98. The provisions of Section 97 (3) of the ECA contain an exhaustive list of bodies authorised to access to traffic and location data. In conjunction with the special regulations governing the activities of the competent authorities, the purpose for which the authorities may request traffic and location data is also always determined. The detailed conditions under which the competent authorities may obtain access are further governed by these specific regulations, some of which have been challenged by the present petition, while others have not. The Constitutional Court examined the appropriacy of the interference with the right to private and family life only by applying the contested legal regulation.

Using Traffic and Location Data in Criminal Proceedings

99. Pursuant to Section 97 (3) of the ECA in conjunction with Section 88a (1) of the Criminal Procedure Code, law enforcement bodies may request traffic and location data in association with the prosecution of criminal offences punishable by a maximum term of imprisonment of at least three years and other specifically listed criminal offences subject to a lighter punishment (primarily related to "cybercrime").

100. Already in the Judgment file reference Pl. ÚS 24/10, the Constitutional Court stated, in relation to the proportionality of the restriction of a fundamental right in the context of data retention, that "it is necessary, in view of the seriousness and the degree of interference with individuals' fundamental right to privacy in the form of the right to information self-determination (in the sense of Art. 10 (3) and Art. 13 of the Charter), which constitutes the use of retained data, the legislature restricts the use of retained data only for the purpose of criminal proceedings for particularly serious criminal offences and only in the case that the pursued objective cannot be achieved otherwise" (similarly, see also the CJEU in the cited judgment in the case of Digital Rights Ireland). In comparison with the institution of interception, the Constitutional Court also criticised the legislature for an unjustified derogation, contrary to its case law. In the Judgment file reference Pl. ÚS 24/11, it further stated: "In other words, even upon satisfying the afore-mentioned condition of necessity, this public interest [in the prevention and prosecution of criminal offences] may not be automatically assigned priority in the collision in question. On the other hand, it should always be considered whether, in respect to the importance of the subject of a particular criminal offence that was allegedly committed, the interest in prosecuting it outweighs the individual's right to decide whether and to whom they will make their personal data available. It is up to the legislature to determine in which cases of criminal offences this public interest prevails, while the decision must take into account their seriousness, similarly to determining sentencing options, for instance. It remains to be added that the same principles are followed in the case of limiting the possibility to enact interception and records of telecommunications operation pursuant to Section 88 (1) of the Criminal Procedure Code only when the criminal proceedings are conducted in respect of a particularly serious criminal offence or in respect of an intentional criminal offence the prosecution of which is mandatory under a promulgated international treaty… "

101. A positive shift can be seen in this respect. The current legal regulation no longer works with the vague concept of "detecting the crime" but offers a specific list of criminal offences. As regards the chosen categorisation, the secondary party, as the proposer of the bill of Act No. 273/2012 Coll., by means of which the contested legal regulation was introduced into the legal order, states: "As regards the category of intentional criminal offences for which the law provides for a maximum prison sentence of at least three years, it is based analogously on the legal regulation of the institute of custody, i.e. the seriousness of the act is derived from the possibility of taking the person into custody. If it is possible to hold a person in custody for offences with the aforementioned sentencing options, which is the most invasive means of criminal law leading to deprivation of liberty, then it is appropriate to obtain traffic and location data under Section 88a of the Criminal Procedure Code."

102. The Constitutional Court insists that the obligation to retain and provide traffic and location data must be seen as an interference with an intensity comparable to that of the interception order and must thus be treated the same. Therefore, using the above perspective, the blanket collection of traffic and location data "in stock" and using the data for approx. 90% of the facts of criminal offences to which in fact Section 88a (1) of the Criminal Code applies should not be perceived as an appropriate limitation of the right to privacy. Nevertheless, it was found in the proceedings before the Constitutional Court that earlier methods of committing (and thus detecting) crime without using electronic communications services are hardly conceivable today. If new forms of committing criminal offences are created and electronic communications services are increasingly being used for this purpose, the Constitutional Court does not give weight to the statistics on crime detection from the years 2010–2014 submitted by the Petitioner solely for this reason – these years cannot be compared to 2019 in terms of the forms of crime and investigative methods used to detect it (see the testimony of JUDr. Bradáčová). However, the presented statistics have no informative value for another reason: in their case, it is only an indication of how many cases of investigated crime were closed in the specific year, i.e. detected; this fact is influenced by a number of factors and an unambiguous correlation between the availability or unavailability of traffic and location data, the selected investigative methods and their success cannot be convincingly concluded from them, according to the Constitutional Court. Consequently, it cannot be concluded whether or not law enforcement bodies may do without the use of traffic and location data (based on the data retention principle).

103. Similarly, the statistics showing the number of requests for records of telecommunications traffic referred to by the Petitioner in support of the allegations of the overuse of traffic and location data in criminal proceedings are inconclusive. The difference between the statistics processed independently of one another by the Czech Telecommunications Office and the Police with different outputs may be explained by a different methodology, as the secondary party explained in its observations. While the Czech Telecommunications Office records every inquiry made for each operator, the Police provide the number of requests according to the number of cases for which they were submitted. If necessary, the Police have to make several inquiries in one case, both in terms of time (e.g. a BTS station listing covering a 12-hour period requires four inquiries) and in terms of the addressee of the inquiry (it is impossible to predict which operator holds relevant data for the Police), as emerged in particular

from the testimony of JUDr. Bradáčová and Col. Šibor. The overuse of traffic and location data by law enforcement bodies was not established in the proceedings before the Constitutional Court.

104. The testimonies of the informed persons have repeatedly shown that the absence of the data retention principle does not mean that traffic and location data are not used in criminal investigations. In the absence of it, the law enforcement bodies only select other available means, leading the Constitutional Court to conclude that the lack of data retention regulation results in less transparency in the conduct of investigative bodies and, paradoxically, a higher risk of misuse of the data available to the operator about the telecommunication traffic. It should be emphasised that all investigative methods of criminal proceedings by nature of the case constitute (more or less) an interference with the privacy of the persons under investigation; therefore, the question remains whether, even in the absence of the data retention principle, the fundamental rights of the individual are truly protected when investigating bodies opt for alternative methods. In other words, there is no guarantee that the privacy of an individual is more protected by the legislature's failure to adopt the data retention principle, since in the unavailability of traffic and location data, the investigating body may choose more invasive investigative methods in terms of the protection of privacy (always using a certain lawful method to obtain the necessary data).

105. In addition, what will not stand the test is the Petitioner's argument that using the traffic and location data is an inefficient tool, as offenders are aware of their actions and are able to avoid electronic traces. Crime investigation and the relationship between investigators and offenders are characterised by the fact that investigators should, as far as practicable, be ahead of offenders and their methods so that they can effectively detect the crime, which is fully applicable to all investigation methods and there is not a single one which offenders would not attempt to circumvent. However, this is not an argument to reject a particular investigation method as ineffective or inefficient (as such).

106. The Court of Justice of the European Union considers only the investigation of "serious crime" to be a legitimate objective of using traffic and location data in association with the detection of crime, yet it does not define this term and provides the Member States with a margin of appreciation (in the context of data retention, it mentions organised crime and terrorism, for example). Although the concept of serious crime contained in the contested provisions of Section 88a (1) of the Criminal Procedure Code is broad, the Constitutional Court finds it appropriate in view of the results of the tested evidence. It has not been demonstrated in the proceedings that the use of traffic and location data as an investigative method was unnecessary or overused. The testimony of JUDr. Bradáčová showed that in terms of the annual caseload of criminal matters, applications for the records of telecommunications traffic are submitted in 3% of cases, which was indirectly affirmed in his testimony by JUDr. Sokol from the Union of Defence Counsels. At the same time, taking into account social and technological developments, more and more crime (and not only cybercrime) is being committed through or with the help of electronic communication services, where investigators in the past found traces "in mud", they now find mainly electronic traces. Therefore, from the perspective of the Constitutional Court, the extent set by the contested Section 88a of the Code of Criminal Procedure may be justified by the need for rapid and effective detection of the crime referred to therein. In the case of an exhaustive list of crimes committed largely in the virtual environment of electronic devices, it is obvious that without access to traffic and location data, this type of crime (cybercrime) would be practically unpunishable and the State, the task of which is to ensure safety and prosecute crime, would become "toothless" in this respect.

107. The contested legal regulation may also be regarded as proportionate in terms of procedural safeguards against the possible misuse of that competence by the law enforcement bodies. The provisions of Section 88a (1) explicitly require that its application be used only if "the objective pursued cannot be achieved otherwise or if its achievement would otherwise be significantly more difficult", thereby complying with the requirement to minimise interference with the fundamental right. Requesting traffic and location data requires the consent of the court (in the pre-trial proceedings, upon the prosecutor's motion) and the court order must also be duly justified under the aforementioned provision. The individual concerned therefore has the guarantee that the legitimacy of their telecommunication data being requested will be assessed by an independent judicial authority and, if the request is unjustified, it will not be granted. In agreement with the Constitutional Court, the CJEU and the ECtHR also have a similar guarantee in their decision-making activities (see the decisions cited in paragraphs 57-62 above).

108. For the safeguards against misuse of retained data to be effective, there must be tools to check retrospectively the legitimacy of the access obtained to specific traffic and location data. Therefore, another measure balancing the intensity of the interference with the individual's privacy in favour of the public interest pursued consists in the obligation of the competent authority to inform the individual concerned about their

traffic and location data being obtained, as regulated in Section 88a (2) of the Criminal Procedure Code (with the exception of justified cases provided for in paragraph 3 of the same provision). The individual may then use the information obtained and turn to the Supreme Court to review the compliance of the procedure of the law enforcement bodies with the law; the individual is thus endowed with an effective means of defence against any arbitrariness of the public authority. In this regard, no systemic failure has been established in the proceedings before the Constitutional Court.

109. In this part of the review, the Constitutional Court concludes that with respect to the above, the regulation contained in Section 88a of the Criminal Procedure code is, in terms of proportionality of the interference with the right to privacy of the person the data of whom are requested by the law enforcement body, acceptable in all respects, i.e. in terms of the extent of the crime, the strictness of the conditions of access to the data requested and the procedural safeguards available to the person concerned for their defence.

Use of Traffic and Location Data under the Police Act

110. The contested provisions of the Police Act have been a part of the legal order since it entered into force, i.e. since 1 January 2009, and have not yet been subject to review by the Constitutional Court (unlike the other contested provisions). Traffic and location data under the Police Act can be used, under the current (contested) legal regulation, in the case of a search for a specific wanted or missing person and for the purpose of identifying a person of unknown identity or identity of a corpse (Section 68 (2) of the Police Act) or in association with the fight against terrorism [Section 71 (a) of the Police Act]. The Constitutional Court assesses the extent of the above-mentioned competences in terms of the purpose as appropriate for the objective pursued. However, the law does not provide for any supervision of an independent body (court) in relation to the access of the Police to retained data, as generally required for the use of traffic and location data by the Constitutional Court, but also by the CJEU and the ECtHR, which could imply that the safeguards against misuse and the possibility of the individual to defend any potential arbitrariness are not satisfactorily addressed in terms of proportionality and thus the interference with the right to privacy is not sufficiently balanced. It should be noted, however, that the Constitutional Court has so far had the opportunity to comment on the appropriateness of the legal regulation on access to retained traffic and location data only in the context of criminal proceedings, to which it also adapted its arguments; nevertheless, the starting points of the regime under the Police Act are different from those of crime investigation.

111. In carrying out its activities, the Police are bound by the Police Act (in particular, Sections 2 and 11 of the Police Act are essential in this context), and in relation to the issue discussed, they are governed by internal management acts [here in particular the Binding Instruction of Police President No. 215/2008, specifying certain more detailed conditions and procedures for processing personal data (on the protection of personal data), the Binding Instruction of the Police President No. 109/2009, on operations centres, the Binding Instruction of the Police President No. 186/2011, on requesting interception and recording of telecommunication traffic and data on telecommunication traffic, the Binding Instruction of the Police President No. 222/2011, issuing the rules of the filing system of the Police of the Czech Republic, the Binding Instruction of the Police President No. 66/2014, on the CPR information system (criminal proceedings records), and the Binding Instruction of the Police President No. 53/2015, on the search].

112. Searching for persons is an organised police activity carried out using search means; searching is a formalised process which cannot be initiated without a specific application. In order to request location data under the "search" provisions of Section 68 of Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended, in an unlawful manner, it would first be necessary to initiate an unlawful search for a specific person. However, this procedure has specific hierarchical rules established by the internal management acts cited above and is subject to internal monitoring activities. Location data can only be requested from an operator to search for a specific wanted or missing person (legally defined terms – see below) and to identify an unknown person or a corpse found only through the Special Activities Unit or the Operational Centre of the Police Presidium upon request approved by direct supervisors and heads of the relevant unit. Upon initiation of the search, an electronic file is created in which the request for the record of location data is included. The entire procedure is documented and is retrospectively verifiable (with the possibility to draw consequences in the case of suspected misuse of requested data). In practice, therefore, there can be no situation in which one particular police officer could arbitrarily obtain the location data of the person concerned without the involvement of other persons. In this respect, no system failure has been established in the proceedings before the Constitutional Court (see Col. Habada's testimony).

113. Pursuant to Section 111 (c) of the Police Act, a wanted person, within the meaning of the Police Act, means a natural person in relation to whom one of the legal grounds for limiting their personal freedom is established, their place of residence is unknown and the Police have initiated the search; the conditions must be complied with cumulatively in order to identify a particular person as wanted, so that related procedures under the Police Act may be activated. Generally, it may be stated that the wanted person avoids fulfilling their obligations stipulated by law or court decision for some reasons (according to the observations of the secondary party, these are most frequently convicted persons who failed to attend to serve their prison sentence).

114. According to letter (d) of the same provision, a missing person means a natural person who can reasonably be believed to be in danger to their life or health, their whereabouts is unknown and the Police have initiated the search. The missing person is presumed to be in a certain manner at risk and their situation is urgent. Police acts are carried out in hours (minutes) and usually for the benefit of the person concerned (or to achieve another legitimate interest, e.g. tracking down the child with whom one parent is hiding). The Constitutional Court, in particular following the tested evidence, agreed with the arguments of the secondary party, namely the concerns about the consequences of delay in the event that it would be necessary to obtain judicial consent. The Court of Justice of the European Union also states in the Judgment in the case of Tele 2 Sverige AB that the required guarantees of access to the data free of any arbitrariness (proper reasoning of the application and review by an independent body) are required except in urgent cases (paragraph 120).

115. In criminal proceedings, another element balancing the interference with the privacy consists in an additional obligation to notify the persons concerned that their data have been provided (see Section 88a (2) of the Criminal Procedure Code). However, it is necessary to agree with the arguments under which prescribing this obligation in the intent of Section 68 (2) of the Police Act would seem absurd, as the missing and found person learns about the processing of their data by the very fact of being found by the Police. Moreover, under Section 68 of Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended, it is possible to request and obtain only location data relating to the determination of the time and place of residence of the person being searched for (section 68 (4) of the Police Act). The scope of the data to which the Police may have access under this provision is thus significantly reduced by the statute compared to the regime of Section 88a of the Criminal Procedure Code, i.e. solely to the necessary extent.

116. Individuals' safeguards against the misuse of competences under Section 68 (2) of the Police Act thus constitute both internal monitoring activities and sanctions aimed at any perpetrator of the unlawful conduct, either at the service level or at the criminal law level, and the individual has the possibility to defend against unlawful search initiation (and thus an unlawful request of location data) by filing an action for protection against unlawful interference in administrative justice (Section 82 et seq. of Act No. 150/2002 Coll., Administrative Procedure Code, as amended), unless the search was initiated within the scope of criminal proceedings.

117. Even in cases of averting an acute terrorist threat [specifically the contested provisions of Section 71 (a) of the Police Act], the law does not require the prior approval of the court or its subsequent supervision to provide access to the competent authority. The statement of reasons points out that obtaining knowledge pursuant to Section 71 (a) of the Police Act approximates the activity of intelligence services and it is only the unit dealing with the prevention and detection of terrorism that will be competent to perform the activity. The absence of judicial supervision in this exceptional case may be justified both by the temporal urgency which may bind the competent police authority when applying the above provision, as well as by the secret nature of the activity of this unit. Therefore, the Constitutional Court does not find that the intensity of interference with the privacy justifies its derogation even in this case. With respect to the sensitivity and severity of the activities carried out by police authorities in detecting terrorist threats, the absence of the obligation to notify the person concerned of access to their traffic and location data may also be approved (similarly to the activities of intelligence services or in the criminal proceedings provided that the conditions under Section 88a (3) 3 of the Criminal Procedure Code have been complied with).

Other Use of Traffic and Location Data

118. Other competent authorities listed in Section 97 (3) of the ECA are the Security Information Service, Military Intelligence and the Czech National Bank. In so far as the special legal regulation referred to in Section 97 (3) of the ECA, which is closely linked to the review of the appropriacy of that authorisation and the conditions under which the above authorities may obtain access to traffic and location data, was not contested (Section 6 to 10 of Act No. 154/1994 Coll., on the Security Information Service, as amended, Sections 7 to 10 of Act No. 289/2005 Coll., on Military Intelligence, as amended by Act No. 273/2012 Coll., and Section 8 of Act

No. 15/1998 Coll., on Supervision in the Capital Market Area and on Amendments and to Other Acts, as amended), the Constitutional Court is not competent to assess the appropriacy of the regulation in relation to these public authorities at this point.

119. In general, it may be stated that if the objective pursued by granting this competence is legitimate (see paragraphs 83 to 85 above), if there are the conditions stipulated in the specific legal regulation for access to traffic and location data and the guarantees of effective protection of them are sufficiently strict, and if they follow the spirit of the conclusions of this judgment, there is nothing to object to the very fact that Section 97 (3) of the ECA specifies among the competent authorities, among others, the authorities mentioned in the previous paragraph.

Implementing Regulation

120. In order to implement all the statutory mechanisms of retaining and providing access to traffic and location data described above, the Ministry of Industry and Trade adopted an implementing decree which is also challenged by the Petitioner. The previous implementing regulation was annulled by Judgment file reference Pl. ÚS 24/10 primarily due to the fact that the legal regulation the implementation of which it served was annulled, while the Constitutional Court did not comment in detail on the very content of Decree No. 485/2005 Coll., on the scope of traffic and location data, the period of their retention and the form and method of their transmission to the bodies authorised to use them.

121. In accordance with the statutory authorisation contained in Section 97 (4) of the ECA, Decree No. 357/2012 Coll. regulates the scope of retained traffic and location data, the form and method of their transmission to the competent bodies, and the method of their disposal. Thus, the Contested Decree does not deviate from the legality limits. The Constitutional Court further assessed the content of the Decree in the spirit of the above conclusions and concluded that the Decree does not exceed the limits of constitutionality (neither does the contested legal regulation). The Decree is a typical by-law of a technical nature which does not impose on the addressees any new obligations not stipulated in the law (see, a contrario, the reservation of the law pursuant to Art. 4 (1) of the Charter). From the Constitutional Court's perspective, the currently effective legal regulation is more detailed and stricter compared to the previous one, complying with the requirements of Judgments file reference. Pl. ÚS 24/10 and sp. Pl. ÚS 24/11. The concepts of traffic data and location data are defined by the Act (see Sections 90 and 91 in conjunction with Section 97 (4) of the ECA); the Decree merely specifies in more detail their content prescribed by the Act (Section 1 and 2 of the Decree). The same conclusion may be reached regarding the regulation of the method of data transmission (Section 3 and Annex of the Decree). The provisions of Section 4 of the Decree finally specify the obligation for operators to dispose of the retained data after the retention period, as set out in the last sentence of Section 97 (3) of the ECA. In a situation where the Constitutional Court does not consider the contested legal regulation to be disproportionate, it does not have a reason to allow this point of the petition either.

VII.

Summary

122. Alongside the growing threat of terrorist attacks, there has been a logical trend to strengthen the powers and tools of investigative public authorities to the detriment of maintaining the existing standard of fundamental rights of individuals. However, this trend has been gradually changing over time and, as a result of the decisions of the constitutional courts, the ECtHR and the CJEU, political representations are beginning to understand the need to strike a balance, by the maintaining of which States would be able effectively and efficiently to comply with the positive obligations, while not interfering with the individuals' rights (in particular the right to privacy and information self-determination under Art. 10 (2) and (3) and Art. 13 of the Charter in this context) more than strictly necessary in a democratic society. The change in the trend towards strengthening personal data protection, or rather re-establishing the lost balance, is demonstrated, inter alia, by the adoption of the GDPR or the preparation of the adoption of the e-privacy regulation governing privacy and electronic communications instead of the existing directive of the same name. The rapid development of information technology cannot be stopped or hampered by any legal regulation; the reach of the Internet and other electronic communication networks is not limited to national borders, as it is a global phenomenon, i.e. a world-wide phenomenon that national legislatures have to address differently and with difficulties. It is necessary to deal with the fact that the active involvement of individuals creates an infinite amount of different data (metadata) and the risk of their misuse increases exponentially – it is thus necessary to adapt the means of personal data protection.

123. The Constitutional Court concluded that within the conditions of today's information society, in which an ordinary individual uses electronic communication services at almost every step and voluntarily accepts that a huge quantity of data are stored about them, it would be unwise to tolerate a situation in which service providers have user data available, while the state apparatus (in justified cases) not. The blanket retention of traffic and location data represents the effort of the State "not to lose momentum in the information society era" and to possess effective tools to carry out its tasks, especially in the field of security of the State and its inhabitants. In principle, therefore, from the perspective of the Constitutional Court, data retention cannot be rejected. From the perspective of the right to privacy, there is no more considerate option in which the State uses the available data in a non-transparent, "stealthy" manner; however, any such consequence cannot be ruled out without any unambiguous legal regulation.

124. In any case, however, the collection and retention of traffic and location data means a particularly serious interference with the privacy of virtually all citizens of the Czech Republic. The principle of data retention consists in the blanket and non-selective collection of a significant amount of data on each completed electronic communication, which intensively limits the privacy of the individual, which is guaranteed to them at the constitutional level by Art. 10 (2) of the Charter and possibly Art. 10 (3) of the Charter in conjunction with Art. 13 of the Charter. On the one hand, any such serious restriction must be of benefit to a strong public interest and, at the same time, it must be minimised as far as possible so that there is a fair balance between it and the pursuit of the legitimate objectives. The interference can be minimised by limiting the use of telecommunication traffic data to the most necessary cases, by setting strict conditions under which data will be retained stored and made available, and by providing every individual with guarantees that in the case of using their data, they will have an effective means of defence available against any potential misuse. Traffic and location data should be perceived as a valuable source of information about the personal life of the person concerned, the misuse of which may have significant effects on the privacy of the individual. Data on telecommunication traffic can often have a more informative value than knowledge of the content of communication, and the analogy to interception (Section 88 of the Criminal Procedure Code) is appropriate in this case; traffic and location data deserve a similar level of regulation in terms of fundamental rights protection.

125. The obligation to collect and retain traffic and location data can only be tolerated for a reasonable period of time. The Constitutional Court concluded that unless a period of six months is manifestly unreasonable, which has not been established in the proceedings in terms of the application practice or comparison with the European Standard, its task is not to substitute the legislature and to determine that a shorter period would be sufficient and how much shorter the period would be the only reasonable. This is the shortest period of the ranges prescribed by the (currently ineffective) Data Retention Directive and does not deviate from the European standard.

126. Another aspect of assessing the appropriacy of data retention regulation in the narrower sense consists the level of security of the retained data. The provisions concerning security were not contested, yet the Constitutional Court had to address this issue as well. Although a stricter regulation may be envisaged, going beyond the general standard of personal data protection laid down in Section 87 et seq. of the ECA, it cannot be inferred from this fact that the level of security is inadequate, thus undermining the privacy of the individual in a disproportionate manner. The cited provisions of the Electronic Communications Act impose a number of obligations on operators, the compliance with which is subject to supervision by independent bodies: the compliance with the statutory obligations is supervised by both the Czech Telecommunication Office and the Office for Personal Data Protection, which has not expressed any complaints in this respect. In the proceedings before the Constitutional Court, it has not been established that system failure has occurred in practice. Therefore, the Constitutional Court did not agree with the Petitioner's allegation that the level of security of traffic and location data would be insufficient in terms of the protection of individuals' privacy.

127. The provisions of Section 88a of the Criminal Procedure Code were not found to be disproportionate, in particular with regard to the context of the current digital age. Nowadays, criminals almost always (and often exclusively) leave an electronic trace behind, even if they do not commit a crime directly through electronic communications services. In order to fulfil the public interest in ensuring the safety of the inhabitants and property values, the State has the task of detecting and preventing crime; in order to be able to carry out this task effectively, it must not "lag behind" the perpetrators in its investigative methods and must have the appropriate technical means at its disposal. The proceedings have not established that Section 88a of the Criminal Procedure Code would be overused or that the list of criminal offences to which it relates would be unnecessary. The determined conditions of access to the data and the procedural safeguards against misuse are sufficiently strict to balance the interference with the privacy of the individual concerned.

128. The contested provisions of the Police Act were subject to the review by the Constitutional Court for the first time; it is obvious that they do not fully comply with the requirements expressed in the Judgment file reference Pl. ÚS 24/10. In the cited Judgment, however, the Constitutional Court did not address the use of traffic and location data outside criminal proceedings. Both provisions foresee situations where any delay may cause irreversible harm to life or health; the absence of judicial supervision is therefore justified in this case. The same applies to the procedural safeguards against misuse that an individual should be provided with, starting with the obligation to inform them of the use of their data.

VIII.

Conclusion

129. In accordance with Section 70 (2) of Act No. 182/1993 Coll., on the Constitutional Court, the Constitutional Court therefore dismissed the petition of the group of Deputies. In the context of the current social and technological development, the legal regulation complies with the requirement of appropriacy of the interference with the right to privacy in the perspective of Art. 10 (2) in conjunction with Art. 10 (3) and Art. 13 of the Charter and the following case law of the Constitutional Court, and it may be interpreted in a constitutionally conforming manner. Each request and the reasoning behind its submission needs to be thoroughly considered by the competent authority and thoroughly reviewed by the court with respect to the specific circumstances of the case under review, rather than limited to assessing merely the compliance with the formal requirements of the request, as required by the existing legal regulation and the case law of the Constitutional Court.

Chairman of the Constitutional Court:
JUDr. Rychetský

Under Section 14 of Act No. 182/1993 Coll., on the Constitutional Court, as amended, Judge Kateřina Šimáčková submitted her dissenting opinion on the Plenum's decision.

Dissenting Opinion of Judge Kateřina Šimáčková

1. I hereby submit my dissenting opinion to the dismissing judgment of the Plenum, as I believe that the contested legal regulation of Act No. 127/2005 Coll., on Electronic Communications and on Amendments to Certain related Acts (Act on Electronic Communications), as amended (hereinafter only as the "ECA) does not withstand the test from the constitutional law perspective, as it fails to provide sufficient guarantees against the leak or misuse of data the collection of which is imposed by the State and allowed by private entities (mobile operators). I am convinced that even the contested regulation of Act No. 273/2008 Coll., on the Police of the Czech Republic, will not withstand the test, as it interferes with the privacy of individuals in a disproportionate manner; the legislature has provided the Police with overly wide access to sensitive data outside the criminal proceedings without proper justification and time grading, depending on the individual situations, for an excessively lengthy "retention period". All this in combination with the impossibility of the individual to control the extent of the collection and use of personal data by means of "data retention" and possibly to subject unreasonable interference with their privacy to a judicial authority or an expert body.

2. When assessing the "data retention" regulation, it is necessary to proceed from the fact expressed in the Plenum's majority opinion (paragraph 49), namely that a detailed personal and communication profile of the individual may be compiled through the information collected. This includes such vital data as political orientation, health, sexual orientation, personal relations, and social status. From the viewpoint of constitutional law protection, these are therefore extremely sensitive personal data. Even sub-constitutional law also considers these personal data to be within the so-called special category of personal data (or sensitive personal data) and attaches to their protection special obligations beyond the protection of other personal data for any entity processing them. The majority opinion of the Plenum (paragraph 50) admits that metadata about the communication made may be more "dangerous" to the privacy of the individual than knowledge of the content of the communication itself, since they are easy to process and analyse, whereas the future behaviour of the individual may be inferred from the processing results. Thus, metadata which are subject to retention and transmission under the contested legislation can provide very comprehensive and extremely sensitive information about the individual, fundamentally affecting their private sphere, personality rights, and the right to information self-determination.

3. To a certain extent, I share the view of the majority that it is not constitutionally unacceptable for metadata to be retained and transmitted for a certain period time to law enforcement bodies or other specifically defined

entities and solely for very specifically defined purposes. The majority opinion is based on the fact that, within the proportionality test, no other measure capable of achieving the same legitimate objective can be found, but at the expense of a milder interference with the fundamental rights and freedoms of individuals. I do not agree with this majority conclusion for the reasons which I will explain later (see paragraph 11 below). I believe that even if any such measure did not really exist, at least additional guarantees and safeguards need to be required to minimise the negative impact on fundamental rights and freedoms. In my opinion, it is therefore essential and crucial for the constitutionality of such metadata collection, retention and transmission to provide a comprehensive and coherent system of safeguards against the unauthorised processing of any such data, their leaks, alteration, corruption or destruction, both accidentally and deliberately.

4. In my view, the contested legal regulation, in particular the contested provisions of the ECA, fails to provide any such coherent system of guarantees. These guarantees are all the more urgent if we take into account the fact that it is the mobile operators and other private service providers, i.e. entities with minimal public scrutiny, primarily pursuing commercial or private interests, to which the State's obligations (collection, retention, security and other handling of data intended, for example, to prosecute crime) are partially delegated without rigorous and preventive supervision.

5. The protection of data or personal data, which metadata can and will usually be (after all, the purpose of processing the data in the context of the contested legal regulation consists primarily in identifying a specific person, such as perpetrators), has long had a general regulation that was previously contained in Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendments to Certain Acts, as amended (hereinafter only as the "Personal Data Protection Act") and relatively recently in particular in Regulation (EU) 2016/679 of the European Parliament and of the Council of 7 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter only as the "GDPR"), which has now been complemented, after a year-long interval, with the implementing Act No. 110/2019 Coll., on Processing Personal Data, which replaced the Personal Data Protection Act. Since the GDPR constitutes an implementation of the right to information self-determination at a sub-constitutional level and thus specifies its nuances, this general regulation needs to be taken into account when the Constitutional Court conducts a proportionality test and considers whether other instruments are available to achieve a legitimate objective which would interfere less with the fundamental rights and freedoms, or if additional safeguards and technical and organisational measures need to ensure the security of the data in question (and if so, which ones) are supposed to be required in terms of the review of the constitutionality.

6. In relation to the above conclusion that metadata may be used to compile a comprehensive communication and social profile of an individual, including their political views, sexual orientation, etc., it cannot be disregarded that under Art. 22 (1) of the GDPR, everyone has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Even though the provisions of Art. 22 (2) (b) of the GDPR provide for an exemption for the processing if it is authorised by law, it requires that the legal regulation lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. Thus, even a sub-constitutional general regulation requires additional guarantees.

7. For inspiration concerning specific additional guarantees, which in my opinion are missing in the contested legal regulation, or they are not provided for with sufficient certainty, thus not guaranteeing a minimum standard of protection for retained data and guarantees for their secure transfer; I consider it appropriate to use in particular Art. 32 of the GDPR, which, among the relevant measures, stipulates for example the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems by requiring, for example, minimum appropriate hardware and software, security of buildings and rooms, security of servers, minimum requirements for access codes and passwords, etc. Obviously, the measures should also comply with the requirements for immediate data recovery in the event of security incidents, as well as requirements for regular testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the data processing security. The legislature should also require mobile operators to carefully supervise persons who have access to sensitive data and monitor preventively their procedures on an ongoing basis. All data processing processes related to the retention and transmission of relevant metadata should also be subject to an impact assessment on the protection of personal data within the meaning of the above legislation and a regular review in this respect.

8. In relation to securing sufficient safeguards, I consider the contested legislation to be problematic in particular due to the transmission of data to public authorities, which should be distinguished from this perspective from

the retention itself, which was also expressed by Dr. Radim Polčák in his testimony. While the actual retention of data also takes place for purely private purposes by the service providers concerned (e.g. telephone operator's marketing activities) and by defining this purpose, the scope of the processed data and the retention period are also limited, the data transmission takes place solely for the purposes of the interference with the individual's privacy (yet pursuing a legitimate goal), and in my opinion, it thus represents a significantly higher risk of data misuse or leak. In this respect, the contested legislation does not, in my view, provide sufficient general guarantees. The constitutionally conforming legal regulation (regardless of whether it is a statute or by-law) should include specific technical measures such as user identity verification tools, access authorisation management tools, tools for recording information systems activity, their users and administrators, tools for the identification and assessment of security incidents, data transmission tools over a private secure network, and organisational measures such as minimum risk management and security policy requirements, security requirements for suppliers, management of relevant infrastructure operations, etc.

9. Therefore, I do believe that in order to comply with the requirement of the constitutionality of the legal regulation under review, the legal safeguards within the meaning of the above should be regulated explicitly, in a sufficiently definite manner, and with the possibility (or the necessity) of their public supervision specifically in the "data retention" context, obviously beyond the scope of the general regulation contained in the GDPR or any other sub-constitutional legal norm which may serve merely as a starting point and the set of key principles owing to the sensitivity of the collected data, their scope, manner of use, and the seriousness of the purposes for which the data are collected.

10. Only sufficiently specific and generally applicable obligations of electronic service providers and competent public bodies to ensure such guarantees may counterbalance the substantial interference with the fundamental rights and freedoms allowed by the legislation under review. Without such explicit guarantees within "data retention", I believe that the contested legislation cannot be found to be constitutionally conforming.

11. The experts interrogated, especially Dr. Radim Polčák, stated that in other European countries, the regulation is different, while fulfilling the desired objective with a similar effectiveness. In particular, one may consider whether it would be possible to retain the relevant metadata for a shorter period of time in combination with a "freezing order", or to retain for a period of 6 months only some metadata to a lesser extent than at present (the testimonies of other experts imply that the Police and other law enforcement bodies mostly use only some types of personal data and for a shorter period of time), to transmit the metadata to the competent bodies in the extent following the seriousness of the individual cases, or to establish and graduate the access to metadata according to the objective the achievement of which is pursued by the competent body, or possibly to opt for any combination of the above restrictions of the blanket "data retention". The very existence of these alternative solutions (and their successful application in everyday practice in other European countries, such as Germany or Slovakia), which provide more respect for fundamental rights and freedoms, demonstrates the unsustainability of the claim that the current "data retention" regulation in the Czech Republic has no alternative and is the only appropriate and necessary means of achieving the legitimate objective in question. For this reason, I disagree with the outcome of the proportionality test as carried out in the plenary judgment. The above-mentioned minimisation principles (limitation by purpose, minimisation of the scope of processed data, limitation of retention period, etc.) are, moreover, basic principles in any processing of personal data and must also apply to "data retention". Personal data must be processed on the basis of the need-to-know principle for achieving the objective, rather than due to the fact that for the competent authority, they may potentially be nice to have and facilitate their work. In a democratic rule of law state based on respect for the rights and freedoms of the individual, the legal regulation must first and foremost respect the privacy and freedom of the individual, and only in exceptional circumstances and as little as possible can it be interfered with. Thus, the point of reference consists in the individual and their natural rights, rather than the need for public authorities to use metadata in this case.

12. I believe that these requirements do not constitute an inherent limitation of law enforcement bodies in fulfilling their important role in any democratic society. However, the majority view seems to be based on the premise expressed by one of the stakeholders – namely the Chief Public Prosecutor Lenka Bradáčová – that in view of the increasing shift of human life (and hence crime as well) into the "world of data", it is necessary that the State have increasingly greater powers to combat crime even in the "world of data" (to the detriment of the individual's freedom, of course). However, I do not consider this conclusion inevitable. Strengthening the powers of law enforcement bodies to the detriment of an individual's freedom is, at any time and in all circumstances, a value choice. It cannot be argued, therefore, that the more "online" people live and also commit crimes there, the more powers the State must have to monitor our lives. Identically, it could be argued quite the opposite that the more our lives shift into the virtual world, the more the protection of individuals' rights and their personality and privacy should apply to the virtual context of which metadata are an integral part. It is this

latter interpretation that corresponds more to how the Constitutional Court is supposed to approach the protection of human rights as the guardian of the constitutionality and the fundamental rights and freedoms of the individual, and through this perspective, balance the protection of the individual's right with the public interest.

13. Although, in principle, I do not dispute the retention and transmission of metadata, I would like to express my disagreement with the conclusion in paragraphs 76, 89 and elsewhere where, in my view, the whole issue is simplified in an inadmissible manner. The principle of "data retention" is accepted by the Plenum with an argument of general willingness to share personal data for marketing purposes. However, this view ignores the fundamental difference between the voluntary sharing of data which data subjects can control and which takes place for the purposes the achievement of which they wish themselves (receiving business offers), and which they can terminate at any time (by withdrawing the consent, leaving the social network, deleting an account, etc.). On the other hand, "data retention" represents the law-enforced blanket collection of all data (except for content), on the basis of which it is possible to create very detailed profiles of the individuals concerned, regardless of the will or at least the knowledge of the data subjects. In addition, not all of their customers grant consent to the operators with the collection of such data (see paragraph 89 of the judgment stating that it is about 70% of customers), while the Constitutional Court is obliged to protect the fundamental rights of all individuals, including those unwilling to approve of their monitoring by the operator.

14. The majority of the Plenum proceeds from the opinion that the annulment of the contested regulation would create a sort of chaos, less transparency, a higher risk of misuse of data, or possibly put the situation in a "legislative shadow". I do not think these concerns are appropriate. The annulment of the contested legal regulation would, of course, give rise to an urgent need to adopt a new regulation, yet the Constitutional Court could, for example, opt for a long suspension of enforceability and imply that it does not contradict the system itself but only the lack of safeguards and data protection and the scope of their use.

15. The arguments on secured institutional guarantees by means of fines from the existing bodies having a large number of other roles or asserting that no abuse of the system has been established before the Constitutional Court will not withstand the test either. The risk of even high penalties has a minimal deterrent potential if this risk is unlikely (it is not the amount of punishment that matters, but its unavoidability). It is even more effective to set up the system in a manner that prevents misuse. However, the majority was satisfied with the potential possibility of sanctions for possible privacy violators beyond the statutory limits and the convincing speeches by three personalities of the Czech Police and the Prosecutor's Office at the oral hearing.

16. Another important reason for greater supervision of the data collected by private companies on the basis of the obligations set out in the ECA and for greater prudence with their collection and use consists not only in the protection of the individual's privacy but also the possibility of misuse outside criminal proceedings. In a similar context of social networks, it is possible to observe how individual policy campaigns use data published by individuals about themselves and monetised by network operators, and how this misuse of the data collected may lead to interference with the free competition of political forces. Already at the turn of the millennium, Paul Schwartz warned that collecting personal data in cyberspace jeopardises not only separate possibility of self-determination of individuals but also deteriorates the quality of deliberative democracy (Schwartz, Paul M. Privacy and Democracy in Cyberspace. Vanderbilt Law Review, 1999, vol. 52, p. 1609). Eliška Wagnerová described it aptly in general in the title of her paper on privacy protection: "Where freedom is supposed to be, privacy has to be" (Právo na soukromí: Kde má být svoboda, tam musí být soukromí [Right to Privacy: Where Freedom is Supposed to Be, Privacy Has to Be]. In: Šimíček, Vojtěch (ed.). Právo na soukromí [Right to Privacy]. Brno: Masaryk University, 2011, p. 49). In the 2016 text, Boehme-Neßler warns that in the long-term perspective, there will be no democracy unless the protection of privacy is guaranteed (Boehme-Neßler Volker. Privacy: a matter of democracy. Why democracy needs privacy and data protection. International Data Privacy Law. 2016, vol. 6, no. 3, p. 222–229).

17. In conclusion, therefore, I summarise that in the light of insufficient safeguards against the misuse of the data collected, the contested legal regulation does not withstand the test, not only in terms of protecting the rights of individuals but also the whole system of our democracy. Our "data retention" regulation, even in comparison with other European countries, fails to adequately protect or appropriately supervise what happens to the metadata at the collecting operator and how they are subsequently transmitted and used by the public authority itself. The State, imposing and authorising private companies to collect the data, does not use all possibilities to prevent their misuse. In addition, the legislature has failed to provide the individual with the opportunity to have control over the extent to which his or her metadata is used by the State, and thus the individual is deprived of the opportunity to defend themselves against any such interference.