Pl.ÚS 45/17 of 14/05/2019 161/2019 Sb.N 76/94 SbNU 19 Data retention III (collection and use of operational and location data on telecommunications traffic) Czech Republic FINDING of the Constitutional Court On behalf of the Republic Finding The Constitutional Court decided in plenary session composed of the president of the court Pavel Rychetský and judges Ludvík David, Jaroslav Fenyk, Josef Fiala, Jan Filip, Jaromír Jirsa (reporting judge), Tomáš Lichovník, Vladimír Sládeček, Radovan Suchánek, Kateřina Šimáčková, Vojtěch Šimíková, Milada Tomková, David Uhlíř and Jiří Zemánka on the proposal of a group of deputies, represented by Mgr. et Mgr. Jan Vobořil, attorney-at-law, with registered office in Prague 7, U Smaltovny 1115/32, on the repeal of the provisions of § 97 paragraphs 3 and 4 of Act No. 127/2005 Coll., on electronic communications and on the amendment of some related laws (Electronic Communications Act) , as amended, § 88a of Act No. 141/1961 Coll., on criminal court proceedings (penal code), as amended, § 68 paragraph 2 and § 71 letter a) Act No. 273/2008 Coll., on the Police of the Czech Republic, and Decree No. 357/2012 Coll., on the storage, transmission and disposal of operational and location data, with the participation of the Parliament of the Czech Republic and the Ministry of Industry and Trade as participants in the proceedings and the government as a party to the proceedings, as follows: The proposal is rejected. Justification I. Definition of the matter 1. The group of 58 deputies (hereinafter also referred to as "the group of deputies" or "the petitioner"), according to Article 87, paragraph 1 letter a) and b) of the Constitution of the Czech Republic (hereinafter referred to as the "Constitution"), by proposal dated 20 December 2017, demands from the Constitutional Court in proceedings pursuant to Section 64 et seq. of Act No. 182/1993 Coll., on the Constitutional Court, as amended, (hereinafter referred to as the "Act on the Constitutional Court") repealing the provisions listed in the title. 2. The proposal challenges some provisions of the legal regulation of the preventive retention of operational and location data on electronic communications by telecommunications service providers (hereinafter also "data retention") and the possibility of their subsequent provision to: a) law enforcement authorities, b) the Police of the Czech Republic (hereinafter also just "police") for the purposes of the launched search for a specific wanted or missing person, establishing the identity of a person of unknown identity or the identity of a found corpse or preventing or detecting specific threats in the field of terrorism, c) Security Information Service, d) Military Intelligence, e) Czech the National Bank for capital market supervision purposes. 3. The challenged legal regulation pursues, as also follows from the relevant explanatory reports, various goals that can also be derived from the list of authorities authorized to deal with stored data. It concerns the security and defense of the state, the protection of persons and property from criminal activity, the search for wanted, missing or lost persons and the supervision of the capital market. The original

legislation establishing the obligation to store operational and location data was adopted in 2005 in response to increasing risks in the area of security related to the increasing use of electronic communication systems, to which it was necessary to adapt the powers of the authorities responsible for the performance of tasks to ensure the security and defense of 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 created or processed in connection with the provision of publicly available electronic communications services or public communications networks and on the amendment of Directive 2002/58/EC (hereinafter referred to as " data retention directive") - by decision of the Court of Justice of the European Union (hereafter referred to as "CJEU") no longer valid today (see below). 4. In order to fulfill the stated objectives, the challenged legal regulation orders the obliged entities (providers of electronic communication services, hereinafter also referred to as "operators") to store "packages of data" about all clients, users of telecommunication services, for a period of six months retroactively. For example, in the case of telephone calls or SMS and MMS messages (including unsuccessful connection attempts), the operator stores data on the telephone numbers of the caller and the called party, the date and time of the start and end of the communication, the location and movement of the user of the given service. In the case of using Internet services and e-mail communication, the operators are also obliged to collect, in particular, user accounts, the identifier of the computer and the searched server (IP address, port number), data on the e-mail address of the participants in the communication and the e-mail protocol. 5. Simply put, on the basis of the challenged legislation, operators store information about every telephone connection, text message, internet connection or e-mail correspondence, i.e. detailed data about all communication, location of communication participants and internet services provided. Some of this data is stored by the operators for their own needs (service billing, complaints, marketing) even without the obligation established by the challenged law. II. Argumentation of the petitioner6. A group of MPs proposes to cancel the challenged legislation, as it unconstitutionally interferes with the right to privacy guaranteed by the Charter of Fundamental Rights and Freedoms (hereinafter referred to as the "Charter") pursuant to Article 7, paragraph 1 of the Charter, to protect against unauthorized interference in private and family life pursuant to Article 10, paragraph 2 of the Charter, the right to protection against unauthorized collection, disclosure or other misuse of personal data pursuant to Article 10, paragraph 3 of the Charter and the right to maintain the confidentiality of messages submitted by telephone or other similar device pursuant to Article 13 of the Charter. The petitioner further objects to the contradiction of the contested regulation with Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms

(hereinafter referred to as the "Convention"). 7. The petitioner introduces her argument by referring to the case law of the Constitutional Court and the Court of Justice of the European Union, which already dealt with the issue of data retention [finding of the Constitutional Court no. stamp Pl. ÚS 24/10 of 22 March 2011 (N 52/60 Coll. 625; 94/2011 Coll.); ruling of the Constitutional Court no. stamp Pl. ÚS 24/11 of 20 December 2011 (N 217/63 Coll. 483; 43/2012 Coll.); judgments of the Court of Justice of the European Union of 04/08/2014 in the joined cases C-293/12 and C-594/12 (Digital Rights Ireland Ltd) and of 12/21/2016 in the joined cases C-203/15 and C -698/15 (Tele2 Sverige AB)]. 8. The proposal primarily claims that the challenged legislation is disproportionate in relation to the constitutionally guaranteed right to privacy, as it does not preserve its essence and meaning according to Article 4, paragraph 4 of the Charter. According to the petitioner, the very monitoring, collection and storage of operational and location data is unconstitutional, as it is widespread and non-selective. The petitioner states that the measure creates a legitimate feeling that everyone is under constant surveillance and does not allow for any distinction. Nowadays, significantly more data is generated than was the case in 2011, when the Constitutional Court last decided on the matter, because the use of data services in mobile ("smart") phones has expanded, which makes it possible to obtain a detailed overview not only of the social ties and habits of an individual , but also about its movement. The petitioner considers the fact that the storage of operational and location data also applies to persons with an obligation of confidentiality - professional secrecy (lawyers, doctors, consultants) to be intolerable. Extensive storage of sensitive data entails the risk of its misuse - data on journalists were misused abroad (Poland) or participants in an anti-government demonstration were determined based on them (Belarus). 9. Furthermore, in relation to the individual contested provisions, the petitioner objects that the definition of the purposes for which operational and location data can be stored under national law is disproportionately broad and, as a result, in violation of Article 15, paragraph 1 of the Directive of the European Parliament and of the Council 2002/ 58/EC of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive), as amended (hereinafter referred to as the "e-Privacy Directive"), as individual privacy can be restricted in this respect only for the purpose of ensuring public safety, defense of the state and for the prevention, investigation, detection and prosecution of criminal offences. The possibility of using traffic and location data by the police in the search for a missing or wanted person cannot by its very nature justify exceptions to privacy protection, just like the Czech National Bank's supervision of the capital market. The petitioner is convinced that the authorization according to the provisions of § 97 paragraph 3 letter b) and letter e) Act No. 127/2005 Coll., on electronic communications and on the

amendment of certain related laws (Electronic Communications Act), as amended, (hereafter referred to as "ZEK") in conjunction with § 68, paragraph 2 and § 71 letter a) of Act No. 273/2008 Coll., on the Police of the Czech Republic, (hereinafter referred to as the "Police Act" or "ZPol") are not in accordance with the legitimate goals exhaustively defined by the cited directive. 10. In a narrower sense, what about the possibility to provide operational and location data to law enforcement authorities pursuant to § 97 paragraph 3 letter a) ZEK in conjunction with § 88a of Act No. 141/1961 Coll., on criminal court proceedings (penal code), as amended (hereinafter referred to as "penal code"), according to the proposer, the measure is not capable of fulfilling the legitimate goal - reduction criminal activity and increasing its clarity. According to the petitioner, it follows from the available police crime statistics for the period 2011-2013 that the possibility of using operational and location data has no effect either on the frequency of criminal activity or on its clarity - for serious crime, the statistical conclusions are identical, which foreign studies are also supposed to prove; law enforcement authorities are able to secure the necessary evidence in other ways as well. Furthermore, the petitioner points to the fact that monitoring of operational and location data can be easily bypassed using various tools, e.g. using an anonymous prepaid phone SIM card, which is well known especially to perpetrators of serious crimes. The result is the monitoring of the communications of the entire company, which does not commit criminal activity, to protect against criminals who know well how to technically avoid monitoring - the measure is thus unsuitable for the fulfillment of a legitimate goal within the proportionality test. In addition, it is clear that the data in question is overused, as it is not only required to clarify a particularly serious crime, but often serves as evidence in ordinary criminal proceedings. 11. In relation to § 97 paragraph 3 letter b) ZEK in conjunction with § 68 paragraph 2 and § 71 letter a) ZPol does not respect the challenged legal regulation, according to the petitioner, the conclusions of the cassation decision no. stamp Pl. ÚS 24/10 (especially point 36), according to which the provision of operational and location data must be preceded by a decision of an independent court, which is not required by law now. In some cases, the police have access to traffic and location data without a court authorization, and are not required to inform the subject of the use of the data or subsequently inform the data subject (as in the case of wiretapping), so the person concerned does not even know that his constitutional rights have been interfered with. III. Active procedural identification and conditions of proceedings 12. According to § 64 paragraph 1 letter b) of Act No. 182/1993 Coll., on the Constitutional Court, a group of at least 41 MPs has the right to submit a proposal for the repeal of the Act or its individual provisions. According to § 64 paragraph 2 letter 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 submit

a proposal for the repeal of another legal regulation or its individual provisions. The proposal in this matter was submitted by a group of 58 deputies and, in accordance with § 64 paragraph 5 of Act No. 182/1993 Coll., on the Constitutional Court, as amended by Act No. 320/2002 Coll., attached a signature document to it, on which each of them individually confirmed that they join the proposal. The petitioner thus fulfills the condition of active legitimacy. 13. The proposal contains all the elements required by law and is admissible in the sense of the provisions of § 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 stop the proceedings according to the provisions of § 67 of the same law. IV. Proceedings before the Constitutional Court14. Pursuant to § 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 parties to the proceedings to comment. According to § 48 paragraph 2 of Act No. 182/1993 Coll., on the Constitutional Court, the President of the Republic, the Ministry of Justice, the Supreme State Attorney's Office and the Office for the Protection of Personal Data were asked to comment on the proposal. 15. The Public Defender of Rights informed the Constitutional Court that she is not participating in the proceedings. The statement of the President of the Republic does not contain any essential (new) facts, therefore the Constitutional Court does not consider it necessary to recapitulate them in more detail. a) Expression of the Chambers of the Parliament16. In their statements, the Chamber of Deputies and the Senate only described the progress of the legislative process of adopting the challenged amendment. 17. Government Draft Act No. 273/2012 Coll., which amends Act No. 127/2005 Coll., on electronic communications and on the amendment of some related laws (Electronic Communications Act), as amended, and some other laws, containing the contested wording of Section 97, Paragraphs 3 and 4 of the ZEK and Section 88a of the Criminal Code, was sent to MPs as print No. 615 on 27/02/2012. The first reading of the draft law was carried out on 14/03/2012, and subsequently the committees recommended that the draft law be approved. The draft law passed the second reading on 14 June 2012. In the detailed debate, MP Jaroslav Krupka spoke with the amendment, who proposed only a legislative-technical change in § 97 paragraph 3 ZEK - the renumbering of footnotes in connection with the adoption of Act No. 142 /2012 Coll., on the amendment of some laws in connection with the introduction of basic registers. The draft law was approved by the Chamber of Deputies as amended in the third reading on 20/06/2012. The Chamber of Deputies forwarded the draft law to the Senate on 26/06/2012, which approved it on the recommendation of all relevant committees in the version adopted by the Chamber of Deputies as Senate Press No. 383 on 18 July 2012. During the meeting

in the Senate, the Minister of the Interior emphasized that the legal regulation of the storage of operational and location data and their use is becoming substantially stricter. The President of the Republic signed the law and it was published in the Collection of Laws on 22 August 2012. 18. The provisions of § 88a of the Criminal Code were further amended by Act No. 455/2016 Coll., which amends Act No. 40/2009 Coll., the Criminal Code, as amended, and other related laws, the government proposal of which was sent to the deputies as Parliamentary Press No. 886 on 16/08/2016. The first reading of the draft law was carried out on 16/09/2016 and 19/10/2016. . 11. 2016. The Senate approved the draft on the recommendation of the Constitutional and Legal Committee in the version adopted by the Chamber of Deputies as Senate Press No. 348 on 30 November 2016. The President of the Republic signed the law and it was promulgated in the Collection of Laws on 29 December 2016. 19. The government's draft law on the police, including the contested provisions of § 68 paragraph 2 and § 71 letter a) was sent to the deputies as print No. 439 on 29/02/2008. The first reading of the draft law took place on 25/03/2008 and subsequently the committees recommended that it be approved in the form of the proposed amendments; the draft law was passed in the second reading on 10 and 18 June 2008. In a detailed debate, nine MPs presented their amendments. The draft law was approved in the wording of the adopted amendments in the third reading on 25/06/2008. The Chamber of Deputies forwarded the proposal to the Senate on 08/07/2008, which approved it for the recommendation of all concerned committees in the wording adopted by the Chamber of Deputies as Senate Press No. 301 on 17/07/2008. The President of the Republic signed the law and on 11/08/2008 it was published in the Collection of Laws. b) Statement of the Ministry of Industry and Trade20. The Ministry of Industry and Trade, which issued the contested Decree No. 357/2012 Coll., on the storage, transmission and disposal of operational and location data (hereinafter referred to as "the Decree"), considers the legislation to be balanced and satisfactory. In support of its position, the Ministry refers to the communication of the Office for the Protection of Personal Data from 2012, which in the interdepartmental comment procedure described the proposal for the relevant amendment to the Electronic Communications Act as adequate with regard to the scope and detail of the amendment and to enshrining the right of a person to be informed about the processing of their personal data data. The Ministry of Industry and Trade further emphasizes that operators, the Czech Telecommunications Authority and the Office for the Protection of Personal Data actively participated in the creation of the decree, drawn up in agreement with the Ministry of the Interior. The decree was created as a compromise between the needs of authorized entities, the technical capabilities of operators and the requirements for privacy protection. c) Statement of the government21. In its statement, the government (hereinafter also

"secondary participant") disagrees with the fact that the contested legislation does not respond to the decisive jurisprudence of the Court of Justice of the European Union and the Constitutional Court. According to the government, the challenged amendment responded adequately to all complaints from the Constitutional Court and nothing can be read into it. In relation to the above-cited judgments of the CJEU Digital Rights Ireland Ltd and Tele2 Sverige AB, the government points out that Czech legislation was not subject to review in either of them; therefore, the judgments could not mean a direct or indirect change for the national legislation. Compared to other European countries, the government considers Czech legislation to be strict and compliant with the requirements of the Court of Justice of the European Union. 22. Using examples from practice, the government demonstrates in which cases the clarification of criminal activity would be impossible without the use of operational and location data stored by law. The government argues that the Electronic Communications Act establishes not only the necessary range of stored data in terms of quantity and time interval, going beyond the scope of data that obliged entities store for their own needs (e.g. service billing), but also a uniform form of processing, without which made access to the requested data difficult. Requirements for the security of stored operational and location data contained in § 88 et seq. The government also considers ZEK to be sufficient. 23. Regarding § 88a of the Criminal Code and the petitioner's objection regarding the overly broad definition of the term serious crime, the government states that the law of the European Union (hereinafter referred to as "EU") does not provide a specific definition and it is up to the member states to interpret the said term . According to the government, a number of restrictions and guarantees were added to the effective wording of Section 88a of the Criminal Code, which already reflect the requirements of the Constitutional Court and the Court of Justice of the European Union and meet the demands placed on the protection of the fundamental rights in question. The government adds that the construction of guarantees and restrictions is almost identical to the demands placed on the use of wiretapping and recording of telecommunications traffic according to Section 88 of the Criminal Code, except for the upper limit of the criminal rate and the subsequent exhaustive list of crimes for which operational and location data can be used. The indispensable added value of the storage of the data in question consists in finding out information about telecommunication traffic that has already taken place, so unlike § 88 of the Criminal Code, it goes into the past - at the same time, it does not touch the content of the communication, which is another essential difference. In the government's opinion, the cited provision would pass all three steps in the proportionality test. 24. Operational and location data represent an important "electronic trace" that plays an irreplaceable role and leads the police to take other effective measures to clarify the crime committed. In addition, according to

the government, the acquisition of operational and location data protects the rights of third parties, as the police can exclude possible suspects based on them and evaluate that there is no longer a need to ask for explanations from a larger number of people, but only from the relevant ones. The government does not share the petitioner's opinion that criminals use mechanisms that ensure the confidentiality of communication, and the challenged tool cannot therefore be considered effective, on the contrary, it considers it an argument in favor of maintaining the obligation to store operational and location data and to make it available to authorized entities under specified conditions. 25. Regarding the alleged abuse of the challenged institute, the government draws attention to the erroneous interpretation of statistics, which is caused by different methods of data processing by the Czech Telecommunications Office and the police. The government, referring to the graphs presented in the statement, rejects the conclusion about the massive detection of operational and location data by law enforcement authorities. 26. The contested provisions of the Police Act are also considered satisfactory by the government. According to Section 68, Paragraph 2 of the said Act, the police is entitled to request data in the event of a search for a wanted or missing person, which are terms defined by law; for this, several conditions must be met cumulatively. The risk of abuse is minimal, the legal regulation is set strictly and is supplemented by equally strict internal acts. The absence of judicial review is justified by the need for a quick response, as the health and life of the persons being sought may be at risk. To § 71 letter a) ZPol regarding the prevention and detection of threats in the field of terrorism, the government adds that, according to statistics, this is a rarely used provision. 27. According to the government, the authorization of the Czech National Bank to obtain operational and location data for the prosecution of administrative offenses in the capital market is based on European legislation and is consistent with it [Art. 69 paragraph 2 letter r) Directive 2014/65/EU of the European Parliament and Council of 15/05/2014 on markets in financial instruments and amending Directives 2002/92/EC and 2011/61/EU]. d) Statement of the Supreme State Attorney's Office28. The opinion of the Supreme State Attorney's Office focuses on the legal regulation of data retention in connection with § 88a of the Criminal Code; it expresses the belief that even if the Constitutional Court were to reach a conclusion on the unconstitutionality of Section 97, Paragraphs 3 and 4 of the ZEK, Section 88a of the Criminal Code would be tenable on its own, just as in the past. According to the Supreme Public Prosecutor's Office, the cited provision meets the requirements of the Court of Justice of the European Union expressed in the Tele2 Sverige AB judgment, as serious criminal activity is defined here sufficiently strictly and other control mechanisms (especially a reasoned court order) are also satisfactory. The Supreme Public Prosecutor's Office disagrees with the petitioner's claim that the abundant use of operational

and location data by law enforcement authorities has no effect on the degree of clarification of criminal activity. According to the Supreme State Attorney's Office, access to data is decisive for the direction and progress (speed, and thus lower costs) of criminal proceedings; one cannot ignore the fact that with the passage of time, criminal activity is becoming more and more sophisticated, it is more often moving to electronic communication platforms (including the Internet) and is committed using them. 29. In the light of the judgments of the CJEU, the Supreme State Attorney's Office finds the legal regulation of the Police Act insufficient, as there is no conditionality for police access to the prior consent of an independent decision-making body on the basis of a reasoned request and the obligation to notify of access to stored data of the person concerned. However, the Supreme State Prosecutor's Office considers the provisions of Section 68, Paragraph 2 of the Criminal Code to be very important for the police. e) Statement of the Office for Personal Data Protection30. In its statement, the Office for the Protection of Personal Data agreed with the proposal to cancel the contested provisions; considers that the criteria newly set in the case law of the CJEU are not taken into account in the Czech legislation. The Office highlights the contribution of the expert group WP 29 [Working group for the protection of natural persons in connection with the processing of personal data established on the basis of Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data (hereinafter referred to as "WP 29")], which already in 2001, in connection with the fight against terrorism, drew attention to the need for a balanced approach in terms of the protection of personal data as part of the fundamental rights and freedoms of the individual. Even then, WP 29 expressed concern about the growing tendency to label the protection of personal data as an obstacle to the effective fight against terrorism and called for counter-terrorism measures not to lower the standard of human rights. 31. In its statement, the Office for the Protection of Personal Data draws attention to the fact that the matter under discussion must also be perceived in the light of the effective Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as "GDPR", the aim of which is to find a balance between the protection of fundamental rights and the development of communication technologies. f) Petitioner's reply32. The Constitutional Court sent the above statements to the petitioner's representative for a reply. The petitioner referred to the argument presented in the proposal for the repeal of the regulations in question and did not consider it necessary to respond further to the comments sent. g) Oral proceedings33. The Constitutional

Court ordered a public oral hearing in the matter in accordance with § 44 of the Act on the Constitutional Court, because in order to better clarify the technical context and details of the issue under discussion, it considered it necessary to conduct evidence by questioning informed persons from among the professional public and persons from practice according to § 49, paragraph 1 of the same Act . Mgr. were summoned to the oral hearing. 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 of the Faculty of Law of Masaryk University), Mgr. Karel Bačkovský (head of the Security and Legal Department, Department of Security Policy of the Ministry of the Interior), JUDr. Tomáš Sokol (president of the Union of Defenders of the Czech Republic, z. s.), senior state attorney JUDr. Lenka Bradáčová and representatives of the police departments concerned (Col. Ing. Vladimír Šibor, director of the Department of Special Activities of the Criminal Police and Investigation Service of the Police Presidium of the Czech Republic; Col. Ing. Bc. Josef Mareš, deputy head of the general crime department of the Regional Directorate of the Police of the Capital City of Prague; Col. František Habada, Head of the Operations Department of the Police Presidium of the Czech Republic). 34. From the interrogation of Mgr. Kellerová The Constitutional Court found that in the past law enforcement authorities required operational and location data even without specific data retention legislation, they only used other legal means to do so (Section 8 of the Criminal Code). At T-Mobile Czech Republic, a. s., data are stored separately in accordance with Section 97, paragraph 3 of the ZEK, and access to them is permitted subject to strict conditions being met; the costs associated with the fulfillment of this legal obligation to the operator are covered by the state. Data for the first three months from the moment of their creation are most often requested. For its own needs (invoicing and service complaints), the operator stores operational and location data (in a range other than that specified by the contested decree, it does not need all of them for its own needs) for a period of two months. For marketing purposes, data can only be stored based on the customer's consent (in the case of T-Mobile Czech Republic, a. s., this is roughly 70% of customers), the operator then stores it for a period of six months. The repeal of the challenged legislation would mean a state of considerable legal uncertainty for operators. 35. From the interrogation of doc. Polčák, it was found that the challenged legislation does not deviate from the European standard; it is conceivable that, for example, stricter requirements for the security of stored data will be set, or graduated access to them according to the seriousness of the crime (not six months flat for all legal purposes). The absence of data retention legislation in some states does not mean that the relevant authorities in them do not use operational and location data to investigate criminal activity, they are only obtained by other means. 36. By questioning Mgr. Bačkovský, it was

proven that during the preparation of the contested amendment proposal, the proceedings were carried out with the knowledge of the findings of the Constitutional Court, no. stamp Pl. ÚS 24/10 and sp. stamp Pl. ÚS 24/11; the creation of a special office where data would be collected was also considered, but the risk of their potential misuse when stored centrally by one institution would be greater. According to him, the definition of criminal activity according to Section 88a of the Criminal Code is sufficiently strict, the use of operational and location data in criminal proceedings is irreplaceable. The use of § 68 paragraph 2 of the Criminal Code serves to protect the life and health of missing persons, a judicial review does not make sense due to the nature of the matter. 37. JUDr. Under questioning, Sokol stated that in his practical experience, recording operational and location data was a marginal issue; it concerns a small number of cases, its informative value is rather supportive, indirect, it is not incriminating evidence. 38. From the interrogation of JUDr. Bradáčová The Constitutional Court found that, due to social and technological developments, the years 2008 and 2019 cannot be compared, as new and more sophisticated ("modern") forms of criminal activity arise every year. Out of the annual idea of criminal cases, requests to record telecommunications traffic concern about 3% of cases. The recording represents a milder measure and often serves as "starting" evidence, which further directs the law enforcement authorities to use more invasive means (especially wiretapping). If the upper limit of the criminal rate in § 88a of the Criminal Code is increased, the mandatory retention of data would not apply to a number of crimes, the investigation of which cannot be dispensed with without operational and location data (spread of drug addiction, dangerous pursuit, dangerous threats, hate crimes, dissemination of an alarm message , child pornography). It is a modern, modern trace, an irreplaceable investigative method that has no adequate equivalent. 39. Interrogation of col. Ing. Šibora, it was found that all requests according to § 88a of the Criminal Code are processed and inquiries to operators are handled nationwide exclusively by the Special Activities Department of the Criminal Police and Investigation Service of the Police Presidium of the Czech Republic (hereinafter referred to as the "Special Activities Department"). Requests are authorized, inquiries made are archived and can be retroactively verified only through the Director of the Special Activities Unit. Dumping of operational and location data is less invasive than wiretapping, often preceding wiretapping authorization. The report on telecommunications traffic (about "withheld data") is an important piece of evidence, but not the only one, it must be supported by other evidence. The activities of the Special Activities Unit are regularly checked by the commission of the Chamber of Deputies (Standing Commission for the control of the use of wiretapping and recording of telecommunications traffic, the use of monitoring of persons and things and interference with the operation of electronic communications) and the Office for the

Protection of Personal Data. 40. From the interrogation of col. Ing. Bc. Mareš learned that traffic and location data recording is often used in serious violent and property crime investigations. While it is an advantage for violent crime that the perpetrator must be physically present at the scene of the crime at some point, this may not be the case for property crime, and then the law enforcement authorities are often left with nothing but electronic traces. The recording of telecommunication traffic also helps to exclude certain selected persons (recidivists) from the list of suspects. In general, it is impossible to say whether a six-month period is necessary or superfluous, it always depends on the circumstances of a specific case. In the period after the first intervention of the Constitutional Court in the area of data retention, 2-3 murders in its district could remain unexplained due to the unavailability of operational and location data. 41. From the interrogation of col. M.Sc. Bc. Habady The Constitutional Court on the application of § 68, paragraph 2 ZPol found that his department manages a central communication system into which missing persons are entered through fourteen regional workplaces that process emergency calls. There is no misuse, localization requests can be verified. In addition, the whistleblower is always personally confronted and "extracted" by the police patrol, so he would change his mind about possible misuse of the investigation. In about half of the cases, the missing person is found exactly where their electronic device was located. In this way, it is possible, for example, to track down persons attempting suicide in time and to avert this consequence. 42. The following conclusion about the state of facts emerged from the evidence provided: The operators adapted to the contested legislation by creating new technical solutions, they did not incur any costs and do not incur them even in connection with processing requests for access to operational and location data, these costs are covered by the state. Access to the data takes place exclusively through the Special Activities Unit, in the regime of the Police Act only the location of the electronic device can be obtained, not all operational and location data as in the case of requests under § 88a of the Criminal Code. The challenged legislation does not deviate from the European standard. Just as technology is developing, so is the form of committing a crime, more and more often only electronic traces are created after the perpetrators, therefore the investigative methods of past years cannot be compared. To date, no system failure has been identified in relation to the storage or disclosure of operational and location data. V. Review of the procedure for adopting contested regulations43. The Constitutional Court, pursuant to § 68 paragraph 2 of Act No. 182/1993 Coll., on the Constitutional Court, as amended by Act No. 48/2002 Coll., reviewed whether the provisions of the Electronic Communications Act, the Criminal Code and the Police Act were challenged received and issued within the limits of the competence established by the Constitution and in the prescribed manner. He came to the conclusion that the legislator

cannot be blamed for anything in this direction - neither the parties to the proceedings nor the intervening parties do not mention any deficits in the legislative process. For brevity, the Constitutional Court refers to the summary of the course of the legislative process in the statements of the chambers of the Parliament. 44. The decree was issued by the Ministry of Industry and Trade. The authority of the ministries to issue legal regulations for the implementation of the law results from Article 79, paragraph 3 of the Constitution, but it is materially conditioned by the existence of explicit statutory authorization and its limits. In the given case, the authorization is the contested provision of Section 97, paragraph 4 of the ZEK - the material condition for the issuance of the by-law is fulfilled. The decree was signed by the Minister of Industry and Trade and duly published in the Collection of Laws with effect from November 1, 2012. VI. Merit review of the proposal45. After reviewing the formal details of the proposal, the flawlessness of the process of adoption of the challenged legal regulations and the evidence provided, the Constitutional Court substantively reviewed the petitioner's objections to the contested legislation and reached the following conclusions. a) General principles The right to privacy, informational self-determination and freedom of communication46. The retention of operational and location data directly affects the constitutionally guaranteed right to privacy in the sense of Article 10, paragraphs 2 and 3, Article 13 of the Charter and Article 8 of the Convention. Privacy is one of the core elements of individual freedom, which is among the most important values of a liberal democracy, and its protection is manifested in many different aspects, as evidenced by the comprehensive embedding of this fundamental right in several different provisions of the Charter. In the present case, it is more specifically the so-called right to informational self-determination (Article 10, paragraph 3 of the Charter) and freedom of communication (Article 13 of the Charter). The right to informational self-determination protects individuals from unauthorized collection, publication or other misuse of their personal data. Freedom of communication protects the secrecy of correspondence and the secrecy of messages carried, whether kept in private, or sent by post, delivered by telephone, telegraph or other device or method. 47. The Constitutional Court explained in detail the general starting points regarding the right to privacy and the admissibility of limiting this right in favor of the constitutionally approved public interest already in the above-mentioned ruling sp. stamp Pl. ÚS 24/10, to which the Constitutional Court refers, especially in points 26 to 40. Only in brief - The Constitutional Court explained in particular that the right to informational self-determination falls among basic human rights and freedoms, because together with personal freedom, freedom in the spatial dimension (domestic) and communication, it completes the personality sphere of an individual, whose individual integrity as the necessary condition for the dignified existence and development of human life in general must be respected

and consistently protected. Respect and protection of this sphere are guaranteed by the constitutional order, as it is an expression of respect for human rights and freedoms (Article 1, paragraph 1 of the Constitution). 48. It is clear from the established jurisprudence of the Constitutional Court, especially in relation to the issue of wiretapping of telephone calls, that the protection of the right to respect for private life in the sense of Article 10 paragraph 3 and Article 13 of the Charter applies not only to the actual content of messages submitted by telephone , but also to data on the numbers called, the date and time of the call, its duration, and in the case of mobile telephony, also the base stations providing the call [cf. e.g. finding sp. stamp II. ÚS 502/2000 of 22 January 2001 (N 11/21 SbNU 83), file no. stamp IV. ÚS 78/01 of 27 August 2001 (N 123/23 SbNU 197), file no. stamp I. ÚS 191/05 of 13 September 2006 (N 161/42 SbNU 327) or sp. stamp II. ÚS 789/06 of 27 September 2007 (N 150/46 SbNU 489)]. The above information about ongoing electronic communication consists of operational and location data. 49. Through the collected information, although the content of the communication is not stored (unlike wiretapping), a detailed record of the individual's movements as well as his personal and communication profile (personal ties, environment, social status, political orientation, state of health or sexual orientation) can be compiled. At the same time, every mobile phone and computer user is an individual, i.e. almost every citizen of the Czech Republic. In the case of Internet services, there is also a very thin, sometimes barely perceptible boundary between operational data and the content itself. 50. The so-called "metadata" about the communication made (i.e. everything except the content) can actually be much more valuable and in fact more "dangerous" than knowing the content of the communication itself, as it is machine-processable and analyzable; the future behavior of the individual can then be inferred from the results of such processing. The content, on the contrary, can actually be "contentless" - if the participants of the communication do not wish it to be comprehensible, they communicate using hints or pre-agreed ciphers. The collection and storage of operational and location data therefore also represent a significant interference with the right to privacy and deserve a similar level of safeguards against misuse from the point of view of the right to privacy as the content of the communication itself. It is therefore necessary to include under the scope of protection of the fundamental right to respect for private life not only the protection of the own content of messages submitted via telephone communication or communication via so-called public networks, but also operational and location data about them (cf. finding file no. Pl. ÚS 24/10). 51. The fundamental right can be limited only on the basis of the law and only to the extent that is necessary in the conditions of a democratic state of law, while maintaining the guarantees of the protection of the individual against manifestations of arbitrariness by the public authorities. The restriction of a fundamental right must above all

correspond to the claims arising from the principle of the rule of law and fulfill the requirements based on the proportionality test - in cases of conflicts between fundamental rights or freedoms with the public interest or with other fundamental rights or freedoms, the purpose (goal) of the intervention must be assessed in relation to the means used , while the criterion for assessment is the principle of proportionality (in a broader sense). The legislation in question must be precise, clear in its wording and sufficiently predictable to provide potentially affected individuals with sufficient information about the circumstances and conditions under which the public authority is authorized to interfere with their privacy (Article 2, paragraph 2 of the Charter), and those possibly they could adjust their behavior so as not to come into conflict with the restrictive norm (Article 2, paragraph 3 of the Charter). The powers granted to the competent authorities, the manner and rules of their implementation must also be strictly defined so that individuals are protected against arbitrary interference. 52. Assessing the admissibility of a given intervention according to the principle of proportionality (in a broader sense) includes three criteria. The first of them is the assessment of the ability to fulfill the purpose (or suitability) - it is determined whether a specific measure is even able to achieve the intended goal, which is the protection of another fundamental right or public good. Furthermore, in the second step, necessity is assessed - it is examined whether the most gentle to the fundamental right was used when choosing the means. Finally, proportionality (in the narrower sense) is assessed, i.e. whether the damage to the fundamental right is disproportionate in relation to the intended goal. Measures restricting basic human rights and freedoms must not, in the case of a collision of a basic right or freedom with the public interest, with their negative consequences exceed the positives that represent the public interest in the adopted measures [cf. find sp. stamp Pl. ÚS 3/02 of 13 August 2002 (N 105/27 Coll. 177; 405/2002 Coll.)]. EU law and the Court of Justice of the European Union53. Pursuant to Article 1, paragraph 2 of the Constitution, the Czech Republic complies with its obligations arising from international law. Union law permeates the Czech legal system through Article 10a of the Constitution, on the basis of which the Czech legislator transferred part of his authority to the EU legislator. The relationship between the constitutional order of the Czech Republic and EU law, of which the jurisprudence of the CJEU is also considered a part, has undergone a certain development over time, on which the Constitutional Court has had several opportunities to comment in the past. 54. The content of Article 1, paragraph 2 of the Constitution in relation to the law of the European Union The Constitutional Court interpreted it in such a way that domestic legislation, including the Constitution, should be interpreted in accordance with the principles of European integration and cooperation of the Union authorities 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 commitment assumed by the Czech Republic in connection with its membership in the European Union, it is necessary to choose a Euro-conform interpretation that supports the implementation of the commitment, not an interpretation that makes implementation impossible [see decision sp . stamp Pl. ÚS 50/04 of 8 March 2006 (N 50/40 Coll. 443; 154/2006 Coll.) or decision no. stamp Pl. ÚS 66/04 of 3 May 2006 (N 93/41 Coll. 195; 434/2006 Coll.)]. In other words, in the area falling within the purview of EU law, it interprets constitutional law taking into account the principles arising from EU law [similarly, see also the decision of no. stamp Pl. ÚS 36/05 of 16 January 2007 (N 8/44 Coll. 83; 57/2007 Coll.)]. All of the above applies while maintaining the limit, which is the so-called material core of the constitutional order, i.e. the essential requirements of a democratic legal state in the sense of Article 9, paragraph 2 of the Constitution [see decision no. stamp Pl. ÚS 19/08 of 26 November 2008 (N 201/51 Coll. 445; 446/2008 Coll.)]. Although EU law is not a reference criterion for assessing the constitutionality of national legislation, and a contradiction with a norm of EU law in itself cannot lead to a derogation from the law, nevertheless, the provisions of EU law and the jurisprudence of the CJEU must be taken into account when interpreting constitutional law. 55. The issue of data retention falls within the purview of EU law, as can be seen from the efforts of the European legislator to establish a uniform framework for national legislation. The Data Retention Directive, on the basis of which the contested legislation was adopted, was declared invalid by the Court of Justice of the European Union, and the new European legislation has not yet been adopted. This created a legislative space vacated by the annulment of the data retention directive, which the member states (including the Czech Republic) can fill - as it is an area of competence shared by them with the EU (not the exclusive competence of the EU) - to the extent that the EU did not implement it or ceased to implement it perform effectively (Article 2, paragraph 2 of the Treaty on the Functioning of the European Union); when filling the vacated legislative space, the legislator of the member state pays attention to the supporting reasons of the judgment of the CJEU, by which the EU regulation in question was invalidated (here, specifically, the judgment of Digital Rights Ireland Ltd). b) Prejudice56. The challenged legal regulation of the Act on Electronic Communications and the Criminal Code was adopted in response to the above-mentioned derogatory rulings of the Constitutional Court no. stamp Pl. ÚS 24/10 and sp. stamp Pl. ÚS 24/11. In subsequent time, the Court of Justice of the European Union also issued the aforementioned judgments of Digital Rights Ireland Ltd and Tele2 Sverige AB. 57. The first of the aforementioned findings sp. stamp Pl. ÚS 24/10 of 22 March 2011, the Constitutional Court annulled the provisions of § 97 paragraphs 3 and 4 ZEK, in the then wording, as well as Decree No. 485/2005 Coll., on the scope of operational and location data, their retention period and

the form and method of their transmission to the authorities authorized to use them. The Constitutional Court applied the jurisprudence of the European Court of Human Rights (hereinafter referred to as "ECtHR") relating to the use of wiretapping (in particular the decision in Malone v UK No. 8691/79 of 2 August 1984) and reiterated its requirements for legal regulation enabling interference with the right to private life by public authority. The European Court of Human Rights considers it necessary to define at the legal level clear rules governing the scope of the use of restrictive measures, to establish minimum requirements for the length and method of storing the obtained information, for its use and access by third parties to it, and to establish procedures for protecting the confidentiality of data and for their destruction ; all so that individuals have sufficient guarantees of protection against their misuse. In § 97 paragraph 3 ZEK, in the original wording, the range of authorized authorities, the purpose of providing operational and location data, and the conditions of their use were not clearly and precisely defined, not even in connection with the special regulations to which the challenged standard referred. The Constitutional Court also criticized the absence of clear and detailed rules containing minimum requirements for the security of stored data (prevention of access by third parties, determination of procedures leading to the protection of confidentiality and data integrity, procedures for their destruction) and guarantees against the risk of their misuse. 58. A few months later, the Constitutional Court, following the decision of stamp Pl. ÚS 24/10 annulled by decision no. stamp Pl. ÚS 24/11 of 20 December 2011 for vagueness and indeterminacy, also § 88a of the Criminal Code. In the proportionality test, the second criterion of necessity was not fulfilled, as the vague and broad formulation of the purpose ("clarification of facts important for criminal proceedings") enabled the request and use of data in essentially any connection with any criminal proceedings. According to the Constitutional Court, the aforementioned deficiency could not be bridged even by a constitutionally compliant interpretation. The Constitutional Court found no reason why the scope of statutory guarantees should differ when using tools according to § 88 of the Criminal Code (wiretapping - future telecommunications traffic including the content of communications) and § 88a of the Criminal Code (operational and location data - telecommunications traffic carried out in the past without content of communication), as in both cases the intensity of interference with the right to privacy is comparable. In addition to the requirements imposed on the legislation in question in the decision no. stamp Pl. ÚS 24/10, the Constitutional Court added here that effective protection against illegal interference with the basic rights and freedoms of the persons concerned should be guaranteed through the obligation to additionally inform users of electronic communication services that their operational and location data have been disclosed to law enforcement authorities . 59. The Court of Justice of the

European Union later, in the Digital Rights Ireland Ltd judgment of 04/08/2014, declared the Data Retention Directive invalid for being in conflict with Article 7 (respect for private and family life) and Article 8 (protection of personal data) of the Fundamental Charter EU rights. Although the directive was able to achieve the objective pursued (harmonization of the regulation of data retention in the field of combating serious crime), even such an objective in itself could not justify that a measure concerning all means of electronic communication and consisting in the retention of data of almost the entire European population was considered necessarily. The Court of Justice of the European Union expressed the requirement of a targeted connection between the stored 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 serious criminal activity in any way, or to persons who, through the retention of their data could for other reasons contribute to the fight against serious crime). 60. Subsequently, the Court of Justice of the European Union, in the Tele2 Sverige AB judgment of 21 December 2016, answered the preliminary questions of Great Britain and Sweden regarding the interpretation of Article 15 paragraph 1 of the e-Privacy Directive in connection with the invalidation of the Data Retention Directive and the resulting consequences for national legislation of the member states. According to Article 15(1) of the e-Privacy Directive, Member States may adopt legislative measures limiting the scope of personal data protection within the meaning of the Directive, if the restriction represents a necessary, reasonable and proportionate measure in a democratic society to ensure national security (i.e. state security), defense, public safety and for the prevention, investigation, detection and prosecution of crimes or the prevention of unauthorized use of an electronic communication system. The Court of Justice of the European Union stated that the cited provision enabling member states to make an exception to the rule of providing protection to personal data must be interpreted restrictively - a situation where the exception becomes the rule cannot be accepted, as is the case with the general and indiscriminate storage of a large amount of data. According to the CJEU, national legislation must effectively define the relationship between the data to be kept and the purpose being monitored, i.e. it must enable the effective definition of the scope of the measure (the range of persons from the public whose data may show at least an indirect connection with serious criminal activity or may contribute to fight against it and to prevent a serious threat to public safety). 61. With another judgment in case C-207/16 of 2/10/2018 (Ministerio Fiscal), the CJEU partially softened the strict tone on the question of the purpose of making operational and location data available; he did not comment on the data retention principle itself. Regarding the Spanish court's preliminary question regarding the interpretation of the same provision as in the previous case - Article 15 of the e-privacy directive - it stated that the disclosure

of data, such as the name, surname and address of the holders of SIM cards activated in a stolen mobile phone, for the purpose of their identification to public authorities power does not interfere with the fundamental rights of these holders enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the EU in such a serious way that access to them in the field of prevention, investigation, detection and prosecution of criminal offenses should be limited only to the fight against serious criminal activity. 62. Recently, the European Court of Human Rights also had the opportunity to recapitulate its jurisprudence relating to wiretapping and, on that occasion, comment on data retention. In the judgment of 13/09/2018, complaints no. 58170/13, 62322/14 and 24960/15, (Big Brother Watch v. the United Kingdom) stated in connection with the provision of communication data a violation not only of Article 8 of the Convention guaranteeing respect for private life, but also Article 10 of the Convention, which guarantees freedom of expression. Violation of Article 8 of the Convention was specifically observed in the request of data on several telephone numbers by the investigating authorities, the purpose of which was to reveal the journalist's source of information (not a goal pursuing a defined public interest) and which was not subject to prior approval by a court or an independent administrative authority. In these two aspects, according to the ECtHR's conclusions, the procedure of the concerned authorities and the applicable legislation of Great Britain were not even compatible with the requirements arising from the presented jurisprudence of the CJEU. In the absence of special legislation that would provide stricter protection for the use of operational and location data in relation to the protection of freedom of the press (activities of journalists), the court also saw a violation of freedom of expression in the light of Article 10 of the Convention. c) Constitutional review of contested legislation63. The issue under discussion must be divided into two levels, which are apparently independent of each other, but in fact, from the point of view of constitutional review, they represent connected vessels. 64. Firstly, it is necessary to answer the question of whether, in the light of the above-explained fundamental rights, it is at all permissible for data of the contested scope to be collected and stored across the board, unaddressed and preventively (Section 97 para. 3 and 4 ZEK and the decree) - therefore, the legal obligation to collect and store operational and location data as such. 65. Secondly, in the case of a positive answer to the first question, it is necessary to deal with the issue of the appropriate definition of the range of authorities authorized to access the collected data in connection with the establishment of legitimate goals, the fulfillment of which the use of operational and location data is intended to serve, including the establishment of legal conditions and guarantees of protection for minimization of interference with the basic rights of individuals [§ 97 para. 3 ZEK, § 88a of the Criminal Code and § 68 para. 2 and § 71 letter a) ZPol]. 66. The Constitutional

Court took into account the arguments of the parties involved, evaluated the evidence, then carried out a proportionality test and came to the conclusion that the current regulation of data retention fulfills the requirements set by the cited earlier jurisprudence of the Constitutional Court and can be applied in a constitutionally compliant manner, i.e. in such a way that it is maximally investigated the rights of individuals guaranteed by Articles 10 and 13 of the Charter. The proposal was therefore rejected for the reasons stated below. Contested legislation67. The provisions of § 97 paragraphs 3 and 4 of the ZEK, in the wording before the amendment implemented by Act No. 287/2018 Coll., reads: Wiretapping and recording of messages § 97 ... (3) A legal or natural person providing a public communication network or providing a publicly available the electronic communications service is obliged to store for a period of 6 months operational and location data that are created or processed when providing its public communications networks and when providing its publicly available electronic communications services. A legal or natural person providing a public communications network or providing a publicly available electronic communications service is only required to store operational and location data related to unsuccessful call attempts if this data is created or processed and stored or recorded at the same time. At the same time, this legal entity or natural person is obliged to ensure that the content of the messages is not stored and forwarded while fulfilling the obligation according to the first and second sentences. A legal or natural person that stores operational and location data is obliged to provide it without delay upon request a) to the law enforcement authorities for the purposes and upon fulfillment of the conditions set by a special legal regulation, b) to the Police of the Czech Republic for the purposes of the launched search for a specific wanted or to a missing person, ascertaining the identity of a person of unknown identity or the identity of a found corpse, preventing or detecting specific threats in the field of terrorism or screening a protected person and upon fulfillment of the conditions laid down by a special legal regulation, c) To the Security Information Service for the purposes and upon fulfilling the conditions laid down by a special legal regulation, d) Military Intelligence for the purposes and upon fulfillment of the conditions laid down by a special legal regulation, e) to the Czech National Bank for the purposes and upon fulfillment of the conditions laid down by a special legal regulation. After the expiry of the period according to the first sentence, the legal entity or natural person that keeps the operational and location data is obliged to dispose of them, unless they have been provided to the authorities authorized to use them according to a special legal regulation or unless this Act provides otherwise (Section 90). (4) Operational and location data according to paragraph 3 are, in particular, data leading to the tracing and identification of the source and addressee of the communication, as well as data leading to the determination of the date, time, method and duration of the communication.

The scope of operational and location data stored in accordance with paragraph 3, the form and method of their transfer to authorities authorized for use according to a special legal regulation, and the method of their disposal shall be determined by the implementing legal regulation. ... 68. Due to its scope, the Constitutional Court does not consider it necessary to state the wording of the decree; for the purpose of justifying the finding, a brief recapitulation of its wording, which specifies the type of stored data, will suffice. According to § 2 of the decree, these are in particular the telephone numbers of the participants of the communication, the date and time of the start of the communication (sending the message), the duration of the communication, in the case of mobile phones, the IMSI identifier (international identifier of the participant of the public mobile communication network assigned by the operator) and the identifier of the mobile device of the participants of the communication. In the case of Internet services, the type of connection, user identification, date and time of Internet connection, access point designation, IP address, and in the case of electronic communication services, also data on connection to an electronic mail box, sending and receiving mail, including addresses of senders and recipients, are stored. Furthermore, the decree regulates the details of the process of providing stored data to the authorized authorities and their disposal after the expiry of the period specified by law. 69. The provision of § 88a of the Criminal Code reads: § 88a (1) If it is necessary for the purposes of criminal proceedings conducted for an intentional crime, for which the law stipulates a prison sentence with an upper limit of the criminal rate of at least three years, for the criminal offense of breaching the secrecy of transported persons messages (Section 182 of the Criminal Code), for the crime of fraud (Section 209 of the Criminal Code), for the crime of unauthorized access to a computer system and information carrier (Section 230 of the Criminal Code), for the crime of measures and storage of an access device and password to a computer system and other such data (Section 231 of the Criminal Code), for the criminal offense of dangerous threats (Section 353 of the Criminal Code), for the criminal offense of dangerous stalking (Section 354 of the Criminal Code), for the criminal offense of spreading an alarm message (Section 357 of the Criminal Code), for criminal the act of incitement to a criminal offense (Section 364 of the Criminal Code), for the criminal offense of approving a criminal offense (Section 365 of the Criminal Code), or for an intentional criminal offense, the prosecution of which is required by an international treaty to which the Czech Republic is bound, to find out data about telecommunications traffic , which are the subject of telecommunications secrecy or to which the protection of personal and intermediary data applies, and if the intended purpose cannot be achieved otherwise or if its achievement would otherwise be significantly more difficult, the president of the court shall order their release in the proceedings before the court, and in the

preliminary proceedings their release to the public prosecutor or the police authority of the judge at the proposal of the public prosecutor. The order to find out data on telecommunications traffic must be issued in writing and justified, including a specific reference to a declared international treaty in the event that criminal proceedings are being conducted for a criminal offense, the prosecution of which is required by this international treaty. If the request relates to a specific user, his identity, if known, must be stated in the order. (2) The public representative or the police authority, by whose decision the matter was finally concluded, and in proceedings before the court the president of the court of first instance after the final conclusion of the case, informs the person of the user mentioned in paragraph 1, if known, about the ordered investigation of data on telecommunications traffic. The information includes the designation of the court that issued the order for the discovery of data on telecommunications traffic and the period to which this order related. Part of the information is instruction on the right to submit, within six months from the date of delivery of this information, to the Supreme Court a proposal to review the legality of the order to ascertain data on telecommunications traffic. The chairman of the chamber of the court of first instance shall submit the information without delay after the final conclusion of the case, the public prosecutor, whose decision the case was finalised, shall submit the information without delay after the expiry of the period for the review of his decision by the supreme prosecutor according to § 174a, and the police authority, whose decision the case was finalised, submits the information without delay after the expiry of the period for review of his decision by the public prosecutor pursuant to § 174 paragraph 2 letter E). (3) Information pursuant to paragraph 2 shall not be submitted by the president of the senate, the public prosecutor or the police authority in proceedings on a crime for which the law provides for a prison sentence with an upper limit of the criminal rate of at least eight years, committed by an organized group, in proceedings on a criminal offense committed for the benefit of an organized criminal groups, in proceedings for the criminal offense of participation in an organized criminal group (Section 361 of the Criminal Code), in proceedings for the criminal offense of participation in a terrorist group (Section 312a of the Criminal Code) or if several persons participated in the commission of the crime and in relation to at least for one of them, the criminal proceedings have not yet been legally terminated, or if criminal proceedings are being conducted against the person to whom the information is to be disclosed, or if the provision of such information could defeat the purpose of this or other criminal proceedings, or could endanger the security of the state , life, health, rights or freedoms of persons. (4) An order according to paragraph 1 is not required if the user of the telecommunications device to which the data on the performed telecommunications operation is to relate gives consent to the provision of data. 70. The provisions of § 68 paragraph 2 and §

71 letter a) ZPol reads: § 68 Search for persons and things... (2) For the purposes of the launched search for a specific wanted or missing person and for the purpose of ascertaining the identity of a person of unknown identity or the identity of a found corpse, the provision of operational and location data from a legal or natural persons providing a public communication network or providing a publicly available electronic communications service in a way that enables remote and continuous access, unless otherwise provided by another legal regulation. The information shall be provided in the form and to the extent determined by another legal regulation. ... § 71 The police department, whose task is to fight terrorism, may, in order to prevent and detect specific threats in the field of terrorism, to the extent necessary, request from a) a legal or natural person providing a public communication network or providing a publicly available electronic communications service to provide operational and location data in a way that enables remote and continuous access, unless otherwise provided by law; information shall be provided in the form and to the extent determined by another legal regulation, ... Principle of data retention71. First of all, according to the Constitutional Court, it is necessary to deal with the question of the permissibility of the general principle of general storage of operational and location data by private entities - as such - from the point of view of the restriction of the fundamental rights in question. The Charter allows restrictions on the personal integrity and privacy of persons by public authority only in exceptional cases - if it is necessary in a democratic society, if the purpose pursued by the public interest cannot be achieved otherwise, and if it is acceptable from the point of view of legal existence and compliance with effective and specific guarantees against at will. 72. The now contested provisions of § 97 paragraphs 3 and 4 of the ZEK and § 88a of the Criminal Code were adopted by Act No. 273/2012 Coll. with effect from 1 October 2012 in response to the finding of stamp Pl. ÚS 24/10. The Constitutional Court, in the cited decision, which annulled the previous version of § 97, paragraphs 3 and 4 of the ZEK, concluded that widespread, preventive collection and storage of data is an interference with the right to privacy and informational self-determination so intense that it is necessary to fulfill the above-mentioned requirements for the admissibility of intervention to set the strictest possible standards - according to the Constitutional Court, the previous legal regulation of the Act on Electronic Communications did not hold up in this regard. The Constitutional Court, in the already cited ruling, as an obiter dictum, expressed doubts about the necessity and adequacy of the tool itself for the widespread and preventive collection of metadata of all electronic communication in terms of the intensity of the intervention in the private sphere of a significant number of individuals, as well as about the fact that sensitive data is concentrated in the hands of private individuals - operators (i.e. service providers in the field of internet and telephone and mobile communication). 73. The legislator

responded to the criticisms of the Constitutional Court by shortening the retention period of operational and location data to six months, explicitly listing the entities authorized to request the stored data, including the purposes for which the authorized entities may request the data, supplementing the legal definition of operational and location data and in again referred to the implementing regulation (challenged decree) for details. 74. In the meantime, the judgment of the CJEU Digital Rights Ireland invalidated the directive on data retention, on the basis of which the principle of data retention was introduced into the Czech legal order (see point 59). In response to this judgment, the Member States then asked the Court of Justice of the European Union preliminary questions regarding the compliance of national regulations on the storage and handling of operational and location data with the Directive on privacy and electronic communications, the most important of which is the judgment of Tele 2 Sverige AB (see point 60) . According to this jurisprudence, the Court of Justice of the European Union found the principle of general and widespread collection of all data on all electronic communications to be contrary to Article 15(1) of the e-Privacy Directive, i.e. to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union guaranteeing the protection of privacy and personal data. At the European level, however, there is no political consensus on the form of a unified regulation of the issue of data retention, which is evidenced by the fact that since the annulment of the data retention directive by the Digital Rights Ireland judgment, there has not yet been a proposal for a new legal regulation that would replace the said directive. Therefore, at the level of national legislation, different approaches of legislators can be encountered. 75. To give an idea of possible alternatives, the Constitutional Court here gives examples of geographically and historically closest, i.e. neighboring, countries. In Germany, after the cassation intervention of the Federal Constitutional Court [finding dated 2 March 2010, file no. stamp 1 BvR 256/08 (BVerfGE 125, 260-385)] new and largely restrictive data retention legislation was adopted. Newly defined categories of operational data can only be stored for ten weeks, location data only for four weeks. Furthermore, there are categories of data that must not be stored at all (in addition to the content of communication, also, for example, data about visited websites and e-mail services); in addition, a "data freeze" mechanism was introduced (collection of future data on the telecommunications traffic of a specific suspect at the initiative of a law enforcement agency). In Slovakia, following the intervention of the Constitutional Court there (finding dated 29/04/2015 file no. PL. ÚS 10/2014), the legislator abandoned the principle of general data storage and instead introduced the "data freeze" mechanism, which is similar to wiretapping in terms of time , as it does not make data available retroactively. In Austria, following the intervention of the Constitutional Court (see decision of 27/06/2014 file no. G 47/2012 and others), the new legislation has not yet been adopted, as there is no political

consensus on the solution to this issue. Only in Poland can currently be found legislation that is more liberal in terms of protecting individual privacy and more benevolent in protecting the security of the state and its inhabitants; the time limit for the retention of metadata is not set by law and prior court approval is not required, statistics on the obtained data are sent to the court only at six-monthly intervals. This amendment is now (also for the second time) the subject of review by the Polish Constitutional Tribunal on the Ombudsman's proposal. 76. The Constitutional Court now returns to the assessment of the admissibility of the principle of data retention as such and states that if it was reluctant to explicitly state the inadequacy of the principle in 2011, it cannot come to such a conclusion today. Since the last decision in the case, development in the field of information technology has advanced significantly, individuals use electronic communications services more and more often, data on telecommunications traffic is created, exists and is stored by operators (private entities with whom customers have concluded private law contracts) for a certain period of time (ensuring the services provided, their subsequent invoicing, complaints, etc.); most customers also give their consent to the processing of their data beyond the scope necessary to provide the requested service (for marketing purposes). It is an undeniable fact that data about an individual's electronic communication will always be collected in some form, even without the legal regulation of data retention (i.e. without the legal obligation to "retain" it), otherwise it would not be possible to carry out electronic communication at all. 77. In other words, operational and location data on electronic communication carried out are not kept only because of a legal obligation, they are and will be kept even without a legal obligation (to a more or less identical extent) , for more or less the same amount of time). As it emerged, for example, from the testimony of doc. Polčák, the absence of a legislatively established principle of data retention in a specific member state does not mean that public authorities do not work with operational and location data, they only get to them through other ways - it cannot be guaranteed that these alternative ways are in terms of interference with the right to privacy less invasive than the legal procedure using the principle of data retention. 78. Therefore, the Constitutional Court logically resolved which of the options represents the "lesser evil" and came to the conclusion that, from the point of view of the transparency of the procedures of public authorities as well as the control over intrusions into the privacy of individuals, a clearly, precisely and sufficiently strictly defined legal framework of the principle is better data retention (see below) than a "legislative shadow" in which both operators would otherwise move when storing operational and location data, as well as public authorities (especially law enforcement authorities) in an attempt to gain access to them. It is a misconception that abandoning the principle of data retention eliminates the risk of misuse of the generated data. 79. It might appear that, with its

current position, the Constitutional Court, as the defender of constitutionality, paradoxically provides the privacy of an individual with a lower degree of protection than the Court of Justice of the European Union, whose primary mission is not the protection of fundamental rights and which takes a position with reference to the protection of privacy to the principle of data retention and a priori (generally) negatively. However, the opposite is true - especially with reference to the demand for predictability, clarity and strictness of legislation affecting the right to privacy. With its approach, the Constitutional Court protects the privacy of the individual more than if, through its intervention, it had created space for the search for other, alternative and less transparent ways to access the metadata of electronic communications. The result of rejecting the principle of data retention would not be a state in which operational and location data would not be generated and would not be stored and used (at least by law enforcement authorities); on the contrary, the consequence would be the loss of public law boundaries and control over the extent of storage of operational and location data, over the method of security and their disclosure. The responsibility for handling operational and location data by public authorities would then de facto be transferred from the state to operators (private persons), which would be an unacceptable situation under the conditions of the rule of law. 80. The Constitutional Court cannot ignore the social and technological development indicated above, which has occurred since its last decision in the case. Interpersonal communication is increasingly shifting its center of gravity to the environment of telecommunications and electronic services. In the current state, it would therefore be unwise to prevent the state, as the bearer of a number of tasks to fulfill the given public interests (here, in particular, the security of the state, the protection of the health and property of the population), from having access to data that can be a valuable source of important information under appropriately set conditions. The principle of data retention as such is therefore not rejected by the Constitutional Court without further ado (just as in the supporting reasons for the decision file no. pl. ÚS 24/10); impose on operators the obligation to collect operational data in real time, moreover, the legislator imposes an obligation arising from the Convention on computer crime, promulgated under No. 104/2013 Coll. m. p. 81. Against the very existence of the principle of data retention, the petitioner argues, among other things, about the threat of professional secrecy (lawyers, social workers, workers of telephone advice centers). It would be possible to attest to this statement, assuming that the purpose for which operational and location data can be requested would not be sufficiently defined, and the conditions of access to them would not be appropriately set, including the guarantees of the persons concerned against the arbitrariness of the authorized authorities (see below). However, in the secure storage of electronic communication data without making them available to an authorized authority, an unreasonable interference in the

privacy of persons bound by confidentiality obligations cannot be seen. In the case of a request for access to confidential electronic communication data - and not only then, 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 goal pursued by the use of traffic and location data prevails (for the fulfillment of a specific public interest), and it is therefore reasonable to make the data available if the interest in protecting the privacy and secrecy of the circumstances of the communication prevails, and to deny access to operational and location data in such a case. 82. In view of the above, the Constitutional Court did not find reasons to comply with the proposal only for the principled reason that the widespread and unaddressed collection of operational and location data on the communication carried out would be a priori disproportionate in relation to the protection of privacy. Therefore, if in the subsequent test of proportionality the conditions for the storage of operational and location data and access to them are found to be sufficiently strict and balancing the limitations of the right to privacy according to Article 10, paragraphs 2 and 3 in conjunction with Article 13 of the Charter, the Constitutional Court does not even then find room for to comply with the proposal. Terms of storage of operational and location dataPurpose of storage and disclosure of operational and location data83. In the first step of the proportionality test, it is necessary to examine whether the legal regulation pursues a legitimate goal and whether the resulting interference with the fundamental right is capable of achieving the set goal. The purpose of the data retention regulation cannot be deduced from the wording of § 97 paragraph 3 of the ZEK itself, but only in combination with § 88a paragraph 1 of the Criminal Code and other regulations that are referred to when determining the authority of individual authorities. In order to define the objective of the contested legislation, it is thus necessary to take into account who has authorized access to the stored data, as this fact is tied to the purpose for which the competent authorities may request access. 84. According to the explanatory report, the goal of collecting operational and location data is their subsequent use for the detection of selected criminal activity (Section 88a, paragraph 1 of the Criminal Code), the search for missing or lost persons (Section 68, paragraph 2 ZPol), for the fight against terrorism [§ 71 letter a) ZPol], activities of intelligence services (obtaining, collecting and evaluating information important for the protection of the constitutional establishment, important economic interests, security and defense of the Czech Republic - see § 2 of Act No. 153/1994 Coll., on the intelligence services of the Czech Republic) and for the supervision of the capital market (§ 8 of Act No. 15/1998 Coll., on supervision in the area of the capital market and on the amendment and addition of other laws, as amended). 85. All the stated goals pursue a strong public interest (protection of the safety and health of the population, the economic

interests of the state) and as such can be characterized as legitimate. The information that the aforementioned authorized authorities obtain from the requested operational and location data is undoubtedly able to move them forward in their activities and direct them one step closer to the fulfillment of the stated purpose, whether it is (simplified and figuratively speaking) clarifying criminal activity, finding the lost elderly or averting a terrorist threat. 86. Furthermore, it is necessary to deal with the question of necessity, i.e. the necessity of limiting the right to privacy in relation to the objective being pursued. The Constitutional Court examined whether there are milder and less invasive means that are also able to achieve the set goal, and came to the conclusion that the use of operational and location data has no real equivalent - there are no means with which the investigated tool could be compared. Although the Constitutional Court compares the use of operational and location data in criminal proceedings in several places in this and earlier findings in terms of the intensity of the interference with the privacy of individual persons to wiretapping, it is not the same thing. While a wiretapping order can monitor a suspect in the future, operational and location data allow authorized authorities to obtain information about an act that has already occurred - such information that authorized authorities cannot otherwise obtain. Equally inappropriate would be the comparison with the monitoring of persons and things according to Section 158d of the Criminal Code, since even here the authorized body obtains maximum information about the movement and communication of the monitored person in real time, but not into the past. For the stated reasons, even the above-mentioned so-called "data freeze" mechanism (point 75), with which some countries (e.g. Slovakia) have replaced the principle of data retention completely or substantially reduced it while simultaneously supplementing the "data freeze" mechanism, cannot be considered an adequate and less invasive substitute " (e.g. Germany) - even here, the authorized body only gains access to data subsequent to the issuance of the relevant order, not to past data. Since there is no means that would allow obtaining the same knowledge as can be read from operational and location data, it is not possible to stop at the second step of the proportionality test, as the contested legislation also meets that. 87. The Constitutional Court therefore shifted the focus of its attention to the last step of the proportionality test, which is measurement - the proportionality of the restriction of the fundamental right to privacy in favor of the pursued goals fulfilling the public interest in the narrower sense of the word. It is necessary to answer whether the affected public interest is important enough to justify the extent of the restriction of the right to privacy by monitoring the electronic communications of almost the entire Czech population for a period of six months "in stock" by commercial entities, whether the contested legislation could not limit the interference with the right to privacy more, that is, whether the legal setting of the conditions is sufficient and whether it

provides enough guarantees against the misuse of this important tool to balance the restrictions. 88. The Constitutional Court focused on sub-problems which, in their summary, have an impact on the assessment of the adequacy of the contested regulation in a narrower sense. Above all, it is necessary to deal with the legal period for which the mandatory data is stored. Furthermore, it must be resolved whether the range of authorities authorized to access the withheld data is set too broadly (in relation to the purpose and the conditions under which they can obtain the data). And finally, it is important whether the individual is provided with sufficient means of protection against misuse of stored data (both in terms of security of stored data and unauthorized access to it, as well as procedural defense tools for the individual in case of suspicion that his data has actually been misused). Retention period of operational and location data89. In relation to the period of six months during which operational and location data are kept pursuant to Section 97, paragraph 3 of the ZEK, the Constitutional Court concluded that its duration represents the mildest variant of the options set by the data retention directive, which was at the time of the adoption of the contested legal modifications still valid. However, it is necessary to ask whether the six-month period is reasonable in today's conditions. From the interrogation of an informed person from among the operators, it was found that the maximum period for which the operator needs to keep the relevant metadata for its own needs does not exceed two months. At the same time, however, the operator stores the selected data (to the extent not identical to the scope established by law) for marketing purposes for a period of six months based on the consent granted by the customer. T-Mobile Czech Republic, a. s., for example, currently stores the data of approximately 70% of its customers in the aforementioned consent regime. 90. At this point, especially in connection with the investigation of criminal activity, it is necessary to distinguish that data is required in two ways in principle. Either the authorized body has data on a specific user (number of his mobile line, fixed line, IP address, IMEI, etc.), in which case he is interested in a list of voice or data services - contacts, activity, or movement of the user (his phone , computers, etc.), or does not know this data, but has information on where the user of interest moved, or where a criminal offense was committed. In the second case, the authorized body is particularly interested in data from individual BTS stations (cells), which will determine, for example, which mobile phones were connected to the given cell at a given moment. 91. From the testimony of Col. Ing. Šibora, during a public oral hearing, the Constitutional Court found that most of the questions refer to the statements of BTS stations, which are usually not older than a few days; an older query for this kind of statement is not even technically possible. Furthermore, from the testimony of Col. Ing. Bc. It emerged from Mareš that, in the case of statements of voice or data services of a specific user, the law enforcement authority

usually uses the maximum possible period of six months. The information obtained from a single statement about telecommunications traffic is often packed with additional knowledge, enabling, for example, the detection of a network of criminals or an organized group. Therefore, without taking into account the specific factual circumstances of the investigated case, it is not possible to accept a generalized conclusion as to how much information obtained for the entire period of six months is necessary or useful for the law enforcement authorities to fulfill the purpose under investigation - it can only be stated that the authorized authorities, in the case of knowledge of the identification data of a specific users use the maximum time allowed by law. However, since the frequency of inquiries about base stations is many times greater than listings of specific subscriber numbers or mobile devices, from the point of view of the total sum of all inquiries, the conclusion is valid that most of the required data is not older than three months (see also Ms. Keller's statement). 92. Although operational and location data older than three months are only used to a limited extent, according to the Constitutional Court, it cannot be concluded that older metadata in specific cases (especially in the application of Section 88a of the Criminal Code) would not be necessary and useful, and thus disproportionate to the objective being pursued . Legislators in response to the finding of stamp Pl. ÚS 24/10 chose a six-month "retention period" as the shortest possible according to the then-current data retention directive. If the Constitutional Court did not accept the conclusion that the principle of data retention would be unconstitutional in itself, and if it was not proven in the proceedings before the Constitutional Court that the retained data were not used or, on the contrary, were overused, i.e. the right to privacy was not investigated by the authorized authorities, it is not possible to reach a conclusion about the inadequacy of the retention period set in this way. There is never a single correct solution to legally regulate a certain area of social relations. Of course, from the point of view of minimizing interference with the privacy of participants in telecommunications traffic, a stricter regulation can be imagined, e.g. - as testified by doc. Polčák - distinguish and grade access to operational and location data according to the goal, the fulfillment of which the authorized body is pursuing, and the derived real need for obtaining data that is just as old (compare the legislation of Belgium, Germany). However, it is up to the legislator what solution he chooses when adjusting the retention period of operational and location data and access to them. If the privacy of the individual is preserved in such a way that the legal regulation of data retention corresponds to the real need for the use of operational and location data, the Constitutional Court does not have the right to interfere with its legislative authority. Security of stored operational and location data93. Legislation protecting the right to privacy to the maximum extent must also require the establishment of clear and detailed rules for securing data storage and

guarantees against their misuse (unauthorized or arbitrary access to them). Especially in the case of data retention, the quantum of data on all users of electronic communication is concentrated in private entities, and therefore the legislator must be doubly strict. It must be clearly established that operational and location data must be stored securely and must not serve the marketing purposes of obliged entities without the express consent of the clients in accordance with the valid personal data protection regulations. However, the dynamic development of the field of information technology also means that the legislator will always be several steps behind; therefore, it may even be beneficial if data security at the legal level is formulated more generally and if the technical details are left to the implementing regulation, which can respond to changes in practice more flexibly and operatively. 94. The security of stored data is contained in § 87 et seq. ZEK (which represent the implementation of the e-privacy directive) together with the general regulations on the protection of personal data - GDPR (subject to Article 95 defining the relationship between the regulation and the e-privacy directive) and the Transposition Act No. 110/2019 Coll., on the processing of personal data. Although the aforementioned passage of the Electronic Communications Act regulating data security has not been challenged, the Constitutional Court cannot resign from evaluating this aspect, because the method of securing stored (provided) operational and location data with a review of the adequacy of the principle of data retention, and therefore also the constitutionality of the contested provisions of § 97 par. 3 and 4 ZEK are closely related. 95. In general terms, it can be stated that the level of security of operational and location data is not lower than the level of security of other data that is processed under the regime of the Electronic Communications Act - see § 88a ZEK (supplemented as well as the challenged provisions by Act No. 273/2012 Coll. . in response to the finding file stamp Pl. ÚS 24/10), as a result of which operational and location data are explicitly ranked at the level of personal data from a security point of view. The law imposes on operators the obligation to secure stored operational and location data and also regulates the mechanism of review and control of compliance with established obligations by independent institutions. Specifically, the operator as a data processor is obliged to: ensure the technical and organizational security of the service provided and to prepare internal technical and organizational regulations to ensure data protection and confidentiality of communications (including the confidentiality of operational and location data associated with communications) [§ 88 para. 1 letter b) in connection with § 89 ZEK]; to inform communication participants about the risk of breaching the security of services, protection of personal data and confidentiality of communications [§ 88 par. 1 letter c) ZEK]; create internal procedures for handling user requests for access to their personal data [§ 88 para. 1 letter d) ZEK]; inform the Office for the Protection of Personal Data about cases of personal data protection

violations, including the method of resolution, and keep records of such cases (Section 88 paragraphs 4 to 7 ZEK); not to process operational and location data for marketing purposes without the consent of the person concerned (§ 90 par. 6 ZEK); to limit to the necessary minimum both the scope of the stored data and the range of persons (authorized employees) authorized to access the stored data and their further processing (Section 90, paragraph 9 and Section 91, paragraph 4 ZEK); maintain confidentiality regarding the request and provision of data in accordance with § 97 paragraph 3 ZEK (§ 97 paragraph 8 ZEK); keep records of cases of disclosure of operational and location data and regularly "report" it to the Czech Telecommunications Authority (§ 97 par. 10 and 11 ZEK). 96. Violation of any of the above obligations by the operator is a misdemeanor [see in particular § 118 paragraph 12 letter a), d) and paragraph 14 letter b) to h), k), z), aa), ae) and paragraph 15 ZEK], for the commission of which in some cases there is a risk of a fine of up to 50,000,000 CZK or up to 10% of the net turnover [§ 118 par. 23 letters c) ZEK], which is the strictest category of sanctions in the misdemeanor regime under the Electronic Communications Act. The Czech Telecommunications Authority is responsible for dealing with offenses under this law, which also has a number of other supervisory powers in relation to operators. Compliance with the general regulations on the protection of personal data during their processing by the operators is also subject to the supervision of the Office for the Protection of Personal Data (§ 87 para. 3, § 88 para. 4 to 7 ZEK). 97. As is clear from the above list, according to the Constitutional Court, the legal order contains a number of guarantees against the misuse of stored data, the level of security of collected data is sufficient; the aforementioned aspect of the investigated issue does not establish the unconstitutional unreasonableness of the contested data retention legislation (especially § 97 par. 3 and 4 ZEK and the decree). In this respect, the conditions of access of the authorized authorities to the requested data (see below) and the fact that the authorized authorities do not have any database of data in which they can search at will are not without significance. Terms of access to operational and location data98. The provisions of § 97 paragraph 3 ZEK contain an exhaustive list of authorities authorized to access operational and location data. In connection with the special regulations governing the activities of the authorized authorities, the purpose for which the authorities may request operational and location data is also always determined. The detailed conditions under which the authorized authorities can gain access are further regulated by these special regulations, some of which have been challenged by the present proposal, while others have not. The Constitutional Court examined the adequacy of the interference with the right to privacy only by applying the contested legislation. Use of operational and location data in criminal proceedings99. Pursuant to Section 97(3) ZEK in conjunction with Section 88a(1) of the Criminal Code, law

enforcement authorities may request operational and location data in connection with the prosecution of criminal offenses punishable by imprisonment with a maximum sentence of at least three years and other specifically listed criminal offenses for which the punishment is less severe (primarily related to "computer crime"). 100. The Constitutional Court already in the decision no. stamp Pl. ÚS 24/10, in relation to the adequacy of the limitation of the fundamental right in the context of data retention, stated that "it is necessary, with regard to the seriousness and degree of interference with the fundamental right of individuals to privacy in the form of the right to informational self-determination (in the sense of Article 10 para. 3 and Article 13 of the Charter), which constitutes the use of stored data, the legislator limited the possibility of using stored data only for the purposes of criminal proceedings conducted for particularly serious criminal offenses and only in the event that the intended purpose cannot be achieved otherwise" (similarly, see also the CJEU in the cited Digital Rights Ireland judgment). In comparison with the wiretapping institute, the Constitutional Court further criticized the legislators for an unjustified deviation, contrary to its jurisprudence. In the finding of sp. stamp Pl. ÚS 24/11 further stated: "In other words, this public interest [in the prevention and prosecution of criminal acts] cannot be given priority in the collision in question every time, even if the above condition of necessity is met. On the contrary, it is always necessary to consider whether, given the importance of the object of a particular criminal offense to be committed, the interest in prosecuting it outweighs the individual's right to decide for himself whether and to whom he discloses his personal data. the decision must, similarly to e.g. in the case of determining the amount of criminal rates, take into account their seriousness. It remains to add that the same principles are also based on the limitation of the possibility to issue an order for wiretapping and recording of telecommunications traffic according to § 88 paragraph 1 of the Criminal Code only for criminal proceedings for a particularly serious crime or for another intentional criminal act, the prosecution of which is required by a promulgated international treaty..." 101. In this regard, a positive shift can be noted. The current legislation no longer works with the vague term "clarification of criminal activity", but offers a specific list of criminal offences. Regarding the chosen categorization of the intervenor as the proposer of the bill no. 273/2012 Coll., by which the contested legislation was introduced into the legal system, states: "As regards the category of intentional crimes for which the law provides for a prison sentence with an upper limit of the criminal rate of at least three years, it is based analogously on the legislation of the institute custody, i.e. the seriousness of the offense is derived from the possibility of taking a person into custody. If for crimes with the specified penalty rate it is possible to take a person into custody, which is the most invasive means of criminal law leading to the deprivation of his personal freedom, then it is appropriate that for such categories of

crimes, it was possible to obtain operational and location data according to § 88a of the Criminal Code." 102. The Constitutional Court insists that the obligation to store and provide operational and location data must be perceived as an intervention comparable in intensity to a wiretapping order and must be approached as such. From the above perspective, the widespread collection of operational and location data "in stock" and the use of this data for approximately 90% of the facts of the criminal offenses to which § 88a, paragraph 1 of the Criminal Code actually applies, should not be perceived as a reasonable restriction of the right to privacy. In the proceedings before the Constitutional Court, however, it was found that the former ways of committing (and therefore also clarifying) criminal activity without the use of electronic communications services can hardly be imagined today. If new forms of criminal activity are constantly emerging and electronic communication services are used more and more for this purpose, the Constitutional Court does not attach weight to the statistics on the detection of criminal activity from the years 2010-2014 presented by the petitioner for this reason alone - the mentioned years cannot be compared with the year 2019 in terms of forms crime and investigative methods used to detect it (see JUDr. Bradáčová's testimony). However, the presented statistics do not have informative value for another reason: In their case, it is only a matter of information on how many cases of investigated criminal activity were terminated in a given year, i.e. clarified; at the same time, a number of factors influence this fact and, according to the Constitutional Court, a clear correlation between the availability or unavailability of operational and location data, the chosen investigative methods and their success cannot be conclusively deduced from them. Therefore, it is not even possible to conclude whether law enforcement authorities can do without the use of operational and location data (based on the principle of data retention) or not. 103. The statistics showing the number of completed requests for statements of telecommunications traffic, which the petitioner cites to support the claim of overuse of traffic and location data in criminal proceedings, are likewise inconclusive. The difference between the outputs of the statistics, processed independently by the Czech Telecommunications Authority and the police with different outputs, can be explained by a different methodology, as the intervenor explained in her statement. While the Czech Telecommunications Office records every inquiry made for each operator, the police report the number of requests according to the number of cases for which they were made. If necessary, the police must make several inquiries in one case, both in terms of time (e.g. a statement of a BTS station covering a period of 12 hours requires four inquiries) and in terms of the addressee of the inquiry (it is not possible to estimate in advance which operator holds the relevant data for the police) , as emerged especially from the testimony of JUDr. Bradáčové and col. Shibora. Abuse of operational and location data by law enforcement authorities in

proceedings before the Constitutional Court was not proven. 104. It has repeatedly emerged from the statements of informed persons that the absence of the principle of data retention does not mean that operational and location data are not used in the investigation of criminal activity. In its absence, the law enforcement authorities only choose other available means, which leads the Constitutional Court to conclude that the consequence of the lack of regulation of data retention is, on the one hand, less transparency of the procedure of the investigating authorities, and, paradoxically, a higher risk of misuse of the operator's data on the telecommunications traffic carried out available. It must be emphasized that all investigative methods of criminal proceedings by their very nature represent (larger or smaller) interference with the privacy of the persons under investigation; therefore, the question remains whether, even in the absence of the principle of data retention, the basic rights of the individual are really being investigated, if the investigating authorities choose alternative methods. In other words, it cannot be guaranteed that the privacy of an individual is more protected by the fact that the legislator did not adopt the principle of data retention, because it is possible that in the case of the unavailability of operational and location data, the investigating authority will choose more invasive investigative methods from the point of view of privacy protection (always some legal way to obtain will find the necessary data). 105. The petitioner's argument that the use of operational and location data is an ineffective tool, because criminals are aware of their actions and can avoid electronic traces, is also untenable. Criminal investigation and the relationship between investigators and offenders is characterized by the fact that investigators should be one step ahead of offenders and their methods as much as possible in order to effectively detect criminal activity. the perpetrators did not attempt to circumvent. However, this is not an argument for rejecting a particular investigative method as ineffective or ineffective (without more). 106. The Court of Justice of the European Union considers only the investigation of "serious criminal activity" as a legitimate aim of using operational and location data in connection with the detection of criminal activity - however, it does not define this term and leaves room for discretion to the member states (in the context of data retention, for example, it mentions organized crime and terrorism). Although the concept of serious criminal activity contained in the contested provision of § 88a, paragraph 1 of the Criminal Code is broad, with regard to the results of the evidence, the Constitutional Court finds it to be reasonable. In the proceedings, it was not proven that the use of operational and location data as an investigative method was unnecessary or that it was overused. From the testimony of JUDr. Bradáčová, it emerged that from the annual idea of criminal cases, requests for the recording of telecommunications traffic concern 3% of cases, which was also indirectly confirmed in his testimony by JUDr. Sokol from the Union of Defenders. At the same time, with regard to social and

technological developments, more and more criminal activities (and not only cyber ones) are committed through or with the help of electronic communication services - where investigators used to find traces "in the mud", now they mainly find electronic traces. Therefore, from the point of view of the Constitutional Court, the scope established by the contested § 88a of the Criminal Code can be justified by the need for quick and effective detection and clarification of the criminal activity mentioned therein. In the case of including an exhaustive list of crimes committed predominantly in the virtual environment of electronic devices, it is clear that without access to operational and location data, this type of crime (cybercrime) would be practically unpunished and the state, whose task is to ensure security and prosecute criminal activity, would become "toothless" in this regard. 107. The challenged regulation can be considered adequate also from the point of view of procedural guarantees against possible abuse of this power by law enforcement authorities. The provisions of § 88a, paragraph 1 of the Criminal Code explicitly request that its application be used only in the case "if the intended purpose cannot be achieved otherwise or if its achievement would otherwise be substantially more difficult", thereby complying with the requirement of minimizing interference with the fundamental right. Requesting operational and location data requires the consent of the court (in the preliminary proceedings to the prosecutor's proposal) and the court order must also be properly justified according to the cited provision. The individual concerned therefore has a guarantee that the legitimacy of the request for his telecommunications data will be assessed by an independent judicial body and, if the request is unfounded, it will not be granted. In agreement with the Constitutional Court, the CJEU and ECtHR also consider a similar guarantee to be pivotal in their decision-making activities (see decisions cited above in points 57-62). 108. In order for safeguards against the misuse of stored data to be effective, there must be tools for retrospectively checking the legitimacy of the obtained access to specific operational and location data. Another measure that balances the intensity of interference with an individual's privacy in favor of the monitored public interest is therefore the obligation of the authorized body to inform the individual concerned about the acquisition of his operational and location data regulated in § 88a paragraph 2 of the Criminal Code (with the exception of justified cases set out in paragraph 3 of the same provision). With the information obtained, the individual can then turn to the Supreme Court, which will review the compliance of the procedure of the law enforcement authorities with the law; the individual is thus endowed with an effective means of defense against the possible arbitrariness of the public authority. In the proceedings before the Constitutional Court, no systemic failure was proven in this regard. 109. In this part of the review, with regard to the above, the Constitutional Court concludes that the regulation contained in § 88a of the Criminal Code is

acceptable in all respects from the point of view of the proportionality of the interference with the right to privacy of the person whose data is requested by the law enforcement authority - as far as the scope of the criminal activity, the strictness of the conditions of access to the required data, as well as the procedural guarantees available to the person concerned for his defense. Use of operational and location data in the regime of the Police Act110. The disputed provisions of the Police Act have been part of the legal system since the beginning of its effectiveness, i.e. since 1 January 2009, and have not yet been subject to review by the Constitutional Court (unlike the other contested provisions). Operating and location data in the regime of the Police Act can be used under the existing (challenged) legislation in the case of a search for a specific wanted or missing person and for the purpose of ascertaining the identity of a person of unknown identity or the identity of a found corpse (§ 68 para. 2 ZPol) or in connection with the fight against terrorism [§ 71 letter a) ZPol]. The Constitutional Court assesses the scope of the above-mentioned authorizations as corresponding to the objective pursued. However, the law does not provide for the control of an independent body (court) over police access to stored data, as is generally required by the Constitutional Court, as well as by the CJEU and ECtHR, for the use of operational and location data, which could evoke the fact that guarantees against abuse and the possibility of an individual to defend themselves potential arbitrariness is not satisfactorily addressed in terms of proportionality, and the interference with the right to privacy is thus not sufficiently balanced. However, it should be noted that the Constitutional Court has so far had the opportunity to comment on the adequacy of the legal regulation of access to stored operational and location data only in the context of criminal proceedings, to which it also adapted its argumentation; however, the starting points of the regime of the Police Act are different from the investigation of criminal activity. 111. In the performance of its activities, the police is bound by the Police Act (especially § 2 and 11 ZPol are essential in the given context), and in relation to the issue under discussion, they are governed by internal procedural acts [here, in particular, the binding instruction of the Chief of Police No. 215/2008 , which establishes some more detailed conditions and procedures for the processing of personal data (on personal data protection), binding instruction of the police chief No. 109/2009, on operational centers, binding instruction of the police chief no. 186/2011, on requiring wiretapping and recording of telecommunications traffic and data on telecommunications traffic, binding instruction of the Police Chief No. 222/2011, which issues the file rules of the Police of the Czech Republic, binding instruction of the Police Chief No. 66/2014, on the ETŘ information system (records of criminal proceedings), and binding instruction of the Chief of Police No. 53/2015, on the search]. 112. Searching for persons is an organized activity of the police carried out with the use of search means; the search

is a formalized process that cannot be initiated without a specific stimulus. In order to be able to request location data under the "search" regime of § 68 of Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended, it would first be necessary to start an unauthorized 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 control activities. Location data can be requested from the operator only for the purpose of searching for a specific wanted or missing person (terms defined by law - see below) and for the purpose of establishing the identity of a person of unknown identity or the identity of a found corpse only through the Special Activities Unit or the Operations Center of the Police Presidium based on an approved request direct supervisor and head of the relevant department. When the search is started, an electronic file is created, in which the request for a listing of location data is based. The entire procedure is documented and is retroactively verifiable - reviewable (with the possibility of drawing consequences in case of suspicion of misuse of the requested data). In practice, there cannot be a situation in which one specific police officer would arbitrarily obtain the location data of a person of interest without the involvement of other persons. In the proceedings before the Constitutional Court, no systemic failure was proven in this regard (see testimony of Col. Habada). 113. According to § 111 letter c) ZPol, a wanted person in the sense of the Police Act means a natural person for whom one of the legal reasons for restricting his personal freedom is given, his place of residence is unknown and a search for him has been announced by the police; the conditions must be met cumulatively in order for a particular person to be marked as wanted and the related procedures under the Police Act to be activated. In general, it can be stated that, for some reason, the wanted person is avoiding the fulfillment of his obligations established by law or a court decision (according to the statement of the intervenor, these are most often convicted persons who have not started serving their prison sentence). 114. According to letter d) of the same provision, a missing person is a natural person whose life or health can be reasonably believed to be in danger, whose whereabouts are unknown and whose search has been announced by the police. A missing person is assumed to be at risk in some way and their situation is urgent. The actions of the police are carried out in a matter of hours (minutes) and usually for the benefit of the person concerned (or to achieve another legitimate interest, e.g. finding a child with whom one of the parents is hiding). The Constitutional Court, especially after the evidence was presented, accepted the arguments of the intervener, specifically the fear of the consequences of a time delay in the event that it would be necessary to obtain court approval. Also, the Court of Justice of the European Union states in the Tele 2 Sverige AB judgment that the guarantees of access to data of a simple will (proper justification of the request and review by an

independent body) are required except in urgent cases (point 120). 115. Another element balancing the invasion of privacy is, in criminal proceedings, the obligation to additionally inform the affected persons that their data has been provided (see § 88a, paragraph 2 of the Criminal Code). However, it is necessary to confirm the argumentation according to which the determination of the said obligation within the meaning of Section 68, paragraph 2 of the Criminal Code would seem absurd, since a wanted and found person learns about the processing of his data by the police precisely when he is found by the police. In addition, in the regime of § 68 of Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended, only location data relating to establishing the time and place of residence of the person being searched for can be requested and obtained (§ 68 par. 4 ZPol). The range of data to which the police may have access according to this provision is thus significantly limited by law, compared to the regime of § 88a of the Criminal Code, and only to the extent necessary. 116. The individual's guarantees against abuse of authority according to § 68, paragraph 2 of the Civil Code thus represent, on the one hand, internal control activities and sanctions resulting from a potential perpetrator of illegal acts either at the level of the employment relationship or at the level of criminal law, and, on the other hand, the individual also has the opportunity to defend himself against an unauthorized search (and thus the unauthorized request of location data) by a lawsuit for protection against illegal intervention in administrative justice (§ 82 et seq. of Act No. 150/2002 Coll., Administrative Code of Court, as amended), if the search was not initiated with the intent of criminal proceedings . 117. Not even in cases of averting an acute terrorist threat [specifically challenged provision § 71 letter a) ZPol] the law does not require the prior consent of the court or its subsequent control for access by an authorized body. In the explanatory report it is stated that the acquisition of knowledge pursuant to § 71 letter a) ZPol approaches the activities of intelligence services, and only the department dealing with the prevention and detection of terrorism will be responsible for the said activity. The absence of judicial supervision in this exceptional case can be justified on the one hand by the urgency of time, which can bind the competent police authority when applying the aforementioned provision, and on the other hand by the secretive nature of the activity of this department. The Constitutional Court therefore does not find the intensity of the invasion of privacy justifying its derogatory ruling here either. The lack of an obligation to inform the person concerned about access to their operational and location data can also be approved, taking into account the sensitivity and seriousness of the activity carried out by the police authorities when detecting terrorist threats (similarly to the activity of intelligence services or in criminal proceedings if the conditions under § 88a are met paragraph 3 of the Criminal Code). Further use of operational and location data118. Other authorized bodies named in § 97 paragraph 3 ZEK are the

Security Information Service, Military Intelligence and the Czech National Bank. Since the special legal regulation to which § 97 paragraph 3 ZEK refers and which is closely related to the review of the question of the adequacy of this authorization and the conditions under which the aforementioned authorities can obtain access to operational and location data is not challenged (§ 6 to 10 of Act No. 154/1994 Coll., on the Security Information Service, as amended; § 7 to 10 of Act No. 289/2005 Coll., on Military Intelligence, as amended by Act No. 273/2012 Coll.; § 8 of Act No. 15 /1998 Coll., on supervision in the area of the capital market and on the amendment and addition of other laws, as amended), the Constitutional Court does not have the right to assess the adequacy of the regulation in relation to the aforementioned public authorities at this point. 119. In general, it can be stated that if the goal pursued by granting this authorization is legitimate (see points 83-85 above), if the conditions of access to operational and location data, as well as the guarantees are effective, set by a special legal regulation the protection of the individual sufficiently strict and if they are carried out in the spirit of the conclusions of this finding, then there is nothing to criticize the fact itself that § 97 paragraph 3 ZEK lists among the authorized authorities, among others, the authorities mentioned in the previous paragraph. Implementation regulation 120. A decree was adopted by the Ministry of Industry and Trade to implement all the above-described legal mechanisms for storing and making operational and location data available, which is also contested by the petitioner. The previous implementing regulation was a finding of stamp Pl. ÚS 24/10 repealed primarily because the statutory regulation, the implementation of which was used, was repealed without the Constitutional Court referring to the very content of Decree No. 485/2005 Coll. their transfer to authorities authorized to use them, expressed in more detail. 121. Decree No. 357/2012 Coll. regulates, in accordance with the legal authorization contained in § 97 paragraph 4 ZEK, the scope of stored operational and location data, the form and method of their transmission to authorized authorities and the method of their disposal. Thus, the contested decree does not deviate from the limits of legality. The Constitutional Court further assessed the content of the decree in the spirit of the conclusions made above and came to the conclusion that the decree does not even exceed the limits of constitutionality (as well as the challenged legal regulation). The decree represents a typical by-law legal regulation of a technical nature, which does not impose any new, non-statutory obligations on the addressees (see a contrario the proviso to the law according to Article 4, paragraph 1 of the Charter). From the point of view of the Constitutional Court, the now effective legal regulation is more detailed and stricter than the previous one, meeting the requirements of findings sp. stamp Pl. ÚS 24/10 and sp. stamp Pl. ÚS 24/11. The concepts of operational data and location data are defined by law (see § 90 and 91 in conjunction with § 97 para. 4 ZEK), the decree only specifies

their legally defined content in more detail (§ 1 and 2 of the decree). The same conclusion can be accepted regarding the modification of the method of data transmission (§ 3 and the annex to the decree). The provisions of § 4 of the decree finally specify the obligation for operators to dispose of stored data after the expiration of the retention period, established by the last sentence of § 97, paragraph 3 of the ZEK. In a situation where the Constitutional Court does not consider the contested legal provision to be disproportionate, it has no reason to comply with this point of the proposed proposal. VII. Summary122. Along with the growing threat of terrorist attacks, a logical trend has developed to strengthen the powers and tools of investigative public authorities at the expense of preserving the existing standard of fundamental rights of individuals. However, the mentioned trend is gradually changing over time, and also as a result of the decisions of the constitutional courts, the ECtHR or the CJEU, political representatives are beginning to understand the need to find a balance, while maintaining which states would be able to effectively and efficiently meet positive obligations, without infringing on the fundamental rights of individuals, in in this context, in particular, the rights to privacy and informational self-determination according to Article 10, paragraphs 2 and 3 and Article 13 of the Charter, interfered more than is absolutely necessary in a democratic society. The change in the trend towards strengthening the protection of personal data, or rather the rediscovery of the lost balance, is demonstrated, among other things, by the adoption of the GDPR or the preparation of the adoption of the so-called e-privacy regulation governing the field of privacy and electronic communications instead of the current directive of the same name. The rapid development of information technologies cannot be stopped or slowed down by any legal regulation; the reach of the Internet and other networks enabling electronic communication is not limited to the borders of individual states, it is a global phenomenon, a worldwide phenomenon that national legislators deal with in different and difficult ways. It is necessary to deal with the fact that an abundance of various data (metadata) is created through the active contribution of individuals and the risk of their misuse increases exponentially - the means of personal data protection must be adapted to this. 123. The Constitutional Court came to the conclusion that in the conditions of today's information society, in which an ordinary individual uses electronic communication services at almost every step and voluntarily accepts that quantities of data are stored about him, it would be unwise to tolerate a situation in which service providers would they had the user data, and the state apparatus (in justified cases) did not. Extensive storage of operational and location data represents the state's effort "not to lose a step in the age of the information society" and to have effective tools in its hands to fulfill its tasks - here especially in the area of the security of the state and its inhabitants. In principle, therefore, from the point of view of the Constitutional Court, data retention

cannot be rejected. From the point of view of the right to privacy, there is no more gentle option in which the state would use the available data in a non-transparent, "penalty" way; however, such a consequence cannot be ruled out without clear legal regulation. 124. In any case, however, the collection and retention of operational and location data means a particularly serious intrusion into the privacy of practically all residents of the Czech Republic. The principle of data retention consists in the widespread, non-selective collection of a significant amount of data on every electronic communication that takes place, thereby intensively limiting the privacy of the individual, which is guaranteed at the constitutional level by Article 10, paragraph 2 of the Charter, and therefore also by Article 10, paragraph 3 of the Charter in connection with Article 13 of the Charter. Such a serious restriction must therefore be beneficial to a strong public interest, and at the same time it must be minimized to the maximum extent possible, so that there is a fair balance between it and the fulfillment of the pursued goals. The minimization of interference can be achieved by limiting the use of telecommunication traffic data to only the most necessary cases, by establishing strict conditions under which the data is both stored and accessed, and by creating guarantees for each individual that, in the event of their data being used, they will have effective means of defense against possible misuse. Traffic and location data should be viewed as a valuable source of information about the personal life of the person concerned, the misuse of which can have significant implications for the individual's privacy. Data on telecommunications traffic can often have a greater informative value than knowledge of the content of the communication, and the analogy to wiretapping (Section 88 of the Criminal Code) is therefore appropriate here; operational and location data deserve a similar degree of regulation from the point of view of the protection of fundamental rights. 125. The obligation to collect and store traffic and location data can only be tolerated for a reasonable period of time. The Constitutional Court came to the conclusion that if the period of six months is not an obviously unreasonable period, which was not proven in the proceedings from the point of view of application practice or by comparison with the European standard, it is not its role to replace the role of the legislator and determine that a shorter period would be sufficient and by how much shorter would be the only reasonable one. This is the shortest period of the range prescribed by the (now invalid) data retention directive, and does not deviate from the European standard. 126. Another aspect of the assessment of the adequacy of the data retention arrangement in the narrower sense is the level of security of the stored data. Provisions related to security were not contested, but the Constitutional Court nevertheless had to deal with this issue as well. Although a stricter regulation can be imagined, going beyond the general standard of personal data protection set out in § 87 et seq. ZEK, it cannot be concluded from this fact that the level of security would be insufficient and would limit

the privacy of the individual in an unreasonable way. The cited provisions of the Act on Electronic Communications establish a number of obligations for operators, compliance with which is subject to the control of independent authorities - supervision of the fulfillment of legal obligations is carried out by both the Czech Telecommunications Authority and the Office for Personal Data Protection, which does not express any specific complaints in this regard. In the proceedings before the Constitutional Court, it was not proven that there was a systemic failure in practice. The Constitutional Court therefore did not confirm the claim of the petitioner that the level of security of operational and location data was insufficient from the point of view of protecting the privacy of individuals. 127. The provisions of § 88a of the Criminal Code were not found to be unreasonable, especially with regard to the context of today's digital age. Criminals today almost always (and often exclusively) leave behind an electronic trail, even if they do not commit a crime directly through electronic communications services. In order to fulfill the public interest in ensuring the safety of residents and property values, the state has the task of detecting, clarifying and preventing criminal activity; in order to be able to perform this task effectively, it must not "falter" behind the perpetrators in its investigation methods and must have adequate technical means at its disposal. In the proceedings, it was not proven that Section 88a of the Criminal Code was overused, nor that the list of crimes to which it applies was unnecessary. The set conditions for access to data as well as procedural guarantees against misuse are sufficiently strict and balance the interference with the privacy of the individual concerned. 128. The contested provisions of the Police Act were subject to review by the Constitutional Court for the first time; it is evident from them that they do not fully correspond to the requirements expressed in the finding sp. stamp Pl. ÚS 24/10. However, in the cited ruling, the Constitutional Court did not deal with the use of operational and location data outside of criminal proceedings. Both provisions foresee situations where any time delay can cause irreversible damage to life or health - the absence of judicial supervision is therefore justifiable here. The same applies to the procedural safeguards against abuse that should be available to the individual, starting with the obligation to inform them about the use of their data. VIII. Conclusion 129. Therefore, in accordance with § 70, paragraph 2 of Act No. 182/1993 Coll., on the Constitutional Court, the Constitutional Court rejected the proposal of the group of deputies. In the context of today's social and technological developments, the legal regulation fulfills the requirement of reasonableness of the interference with the right to privacy in the light of Article 10(2) in conjunction with Article 10(3) and Article 13 of the Charter and subsequent jurisprudence of the Constitutional Court and can be interpreted constitutionally manner. Each request and the rationale for its submission must be thoroughly considered by the authorized body and carefully reviewed by the court with regard to the

specific circumstances of the case under consideration and not limited to assessing the fulfillment of the formal requirements of the request, as required by current legislation and the jurisprudence of the Constitutional Court . Different opinionsDifferent opinion of judge Kateřina Šimáčková1. I take a different position on the rejection decision of the plenary session, because I believe that the challenged legal regulation of Act No. 127/2005 Coll., on electronic communications and on the amendment of some related laws (Electronic Communications Act), as amended, (hereinafter referred to as "ZEK ") is untenable from a constitutional point of view, as it does not provide sufficient guarantees against the leakage or misuse of data, the collection of which the state imposes, and thus enables, private entities (mobile operators). I am convinced that even the contested amendment of Act No. 273/2008 Coll., on the Police of the Czech Republic, will not stand, because it interferes with the privacy of individuals in a disproportionate way; because the legislator gave the police too broad access to sensitive data outside of criminal proceedings without proper justification and too long "retention periods" based on individual situations. All this in combination with the impossibility of the individual himself to control the scope of the collection and use of data about his person through "data retention" and possibly to subject unjustified interventions to his privacy to the control of a judicial authority or an expert body. 2. When assessing the "data retention" adjustment, it is necessary to start from the fact expressed in the majority opinion of the plenary session (point 49), namely that a detailed personal and communication profile of an individual can be compiled through the collected information. And that includes such essential data as political orientation, state of health, sexual orientation, personal ties and social status. From the point of view of constitutional protection, this is extremely sensitive personal data. Even sub-constitutional law considers these personal data to be so-called special categories of personal data (or sensitive personal data) and with their protection links special obligations beyond the protection of other personal data for all those who process them. The majority opinion of the plenary session (point 50) admits that metadata about the communication carried out can be more "dangerous" for an individual's privacy than knowledge of the content of the communication itself, as it is easy to process and analyze, and the future behavior of the individual can then be inferred from the results of such processing. Metadata, which is the subject of storage and transfer on the basis of the challenged legislation, can therefore reveal very complex and extremely sensitive information about an individual, which fundamentally interferes with his private sphere, personal rights and the right to informational self-determination. 3. To a certain extent, I agree with the opinion of the majority that it is not constitutionally unacceptable for metadata to be kept for a certain period of time and transferred to law enforcement authorities, or to other specifically defined entities, and only for very

precisely defined purposes. The majority opinion is based on the fact that, within the proportionality test, no other measure can be found that would be capable of achieving the same legitimate goal, but at the cost of less interference with the fundamental rights and freedoms of individuals. I do not agree with this conclusion of the majority for reasons which I will explain later (see point 11 below). I believe that even if such a measure really did not exist, it is necessary to demand at least additional guarantees and safeguards minimizing the negative impact on fundamental rights and freedoms. In my opinion, it is essential and crucial for the constitutionality of such metadata collection, storage and transmission that a comprehensive and coherent system of guarantees against the unauthorized processing of such data, its leakage, alteration, damage or destruction, both accidental and targeted, is provided. 4. I am of the opinion that the challenged legislation, especially the challenged provisions of the ZEK, do not provide such a coherent system of guarantees. These guarantees are lacking all the more if we take into account the fact that it is precisely mobile operators and other private service providers, i.e. entities with minimal public control pursuing primarily commercial or private interests to which, without consistent and preventive control, the obligations belonging to the state are partially transferred (acquisition, storage, security and other handling of data intended to be used, for example, for the prosecution of criminal activity). 5. Data protection, or personal data, which metadata can certainly be and usually will be (after all, the purpose of their processing in the context of the challenged legislation is mainly to identify a specific person, e.g. a criminal), has for a very long time had a general regulation, which was previously contained in Act No. 101 /2000 Coll., on the protection of personal data and on the amendment of certain laws, as amended (hereinafter referred to as the "Act on the Protection of Personal Data") and, relatively recently, in particular in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 of April 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (general regulation on the protection of personal data) - hereinafter referred to as "GDPR", which is now finally supplemented by an implementing Act No. 110/2019 Coll., on the processing of personal data, which replaced the Act on the Protection of Personal Data. Since the GDPR represents the implementation of the right to informational self-determination at the sub-constitutional level and therefore specifies its nuances, this general regulation needs to be taken into account when the Constitutional Court performs a proportionality test and considers whether other less intrusive tools are available to achieve a legitimate goal to fundamental rights and freedoms, or whether additional guarantees and technical and organizational measures to ensure the security of the data in question should not be required from the point of view of constitutionality review (and if so, what kind). 6. In relation to

the above-mentioned conclusion that it is possible to compile a comprehensive communication and social profile of an individual from metadata, including his political opinions, sexual orientation, etc., it cannot be overlooked that according to Article 22, paragraph 1 GDPR, everyone has the right not to be the subject of any a decision based exclusively on automated processing, including profiling, which has legal effects for him or significantly affects him in a similar way. The provisions of Article 22 paragraph 2 letter b) GDPR provides an exception for such processing if it is carried out on the basis of the law, however, it requires that this legal regulation establishes appropriate measures ensuring the protection of the rights and freedoms and legitimate interests° of the data subject. Even sub-constitutional general regulation thus requires additional guarantees. 7. For inspiration regarding specific additional guarantees, which, in my opinion, are missing in the challenged legal arrangement, or are not set out in it with sufficient certainty, and thus the minimum standard of protection of stored data and guarantees for their safe transfer are not guaranteed, I consider it appropriate to use in particular Article 32 of the GDPR, which among the relevant measures stipulates e.g. pseudonymization and encryption of data, the ability to ensure continuous confidentiality, integrity, availability and resilience of systems by requiring, for example, minimum appropriate technical equipment and software, security of objects and rooms, server security, minimum requirements for access codes and passwords, etc. Requirements for immediate data recovery in the event of security incidents should also be a matter of course, as well as requirements for regular testing, assessment and evaluation of the effectiveness of established technical and organizational measures to ensure the security of data processing. The legislator should also require mobile operators to carefully supervise persons who have access to sensitive data, and to check their procedures as a preventive measure on an ongoing basis. All data processing processes related to the storage and transfer of relevant metadata should also be subject to a personal data protection impact assessment in the sense of the aforementioned legislation and to a regular review from this point of view. 8. In relation to the provision of sufficient guarantees, I also consider the contested legislation to be problematic, especially the transfer of data to public authorities, which from this point of view needs to be distinguished from the storage itself, which was also expressed in his testimony by doc. Radim Polčák. While the actual storage of data also takes place for the purely private purposes of the relevant service providers (e.g. marketing activities of the telephone operator) and defining this purpose also limits the scope of the processed data and the length of their retention, the transfer of data occurs solely for the purpose of encroaching on the privacy of an individual (even if pursuing a legitimate goal), and thus represents a significantly higher risk in terms of misuse or data leakage. In my opinion, the challenged legislation does not provide sufficient

generally valid guarantees in this regard. Constitutionally compliant legal regulation (and regardless of whether at the statutory or sub-statutory level) should contain specific technical measures such as tools for verifying the identity of users, tools for managing access rights, tools for recording the activity of information systems, their users and administrators, tools for identification and evaluation of security incidents, tools for ensuring data transmission using a non-public secure network and organizational measures such as minimum requirements for risk management and security policy, security requirements for suppliers, management of the operation of the relevant infrastructure, etc. 9. Therefore, I believe that there could be a requirement the constitutionality of the reviewed legislation has been satisfied, the guarantees in the sense of the above should be regulated explicitly, with sufficient certainty and with the possibility (or necessity) of their public control specifically in the context of "data retention", and of course beyond the scope of the general regulation contained in the GDPR or in other sub-constitutional legislation, which due to the sensitivity of the data collected, its scope, method of use and seriousness of the purposes for which the data are collected, can only serve as a starting point and a set of basic principles. 10. Only sufficiently specific and generally applicable obligations of electronic service providers and authorized public authorities to ensure these guarantees can balance the fundamental interference with fundamental rights and freedoms that the reviewed legislation enables. Without such explicit guarantees in the framework of "data retention", I believe that the challenged legislation cannot be found to be constitutionally compliant. 11. Learned persons who were interviewed, especially doc. Radim Polčák, stated that in other European countries the regulation is different, while fulfilling the desired goal with similar efficiency. In particular, one can think about whether it would not be possible to store the relevant metadata for a shorter period of time in combination with a "freezing order", or to store only some metadata for a period of 6 months to a smaller extent than is the case today (it follows from the testimony of other informed persons that the police and other law enforcement authorities mostly use only certain types of personal data and for a shorter period of time), transfer metadata to the relevant authorities to the extent of the seriousness of the relevant criminal activity, the access of individual persons or authorities according to the seriousness of the respective cases, or to establish and grade access to metadata according to the goal, the achievement of which the authorized body is pursuing, or to choose any combination of the listed restrictions of general "data retention". The very existence of these alternative solutions (and their successful application in everyday practice in other European countries, for example in Germany or Slovakia), which save more on basic rights and freedoms, points to the unsustainability of the claim that the current regulation of "data retention" in the Czech Republic it has no alternative and is the only appropriate and necessary

means to achieve the relevant legitimate end. For this reason, I therefore disagree with the result of the proportionality test as carried out in the plenary finding. The minimization principles mentioned above (restriction of purpose, minimization of the scope of processed data, limitation of storage time, etc.) are, after all, basic principles for any processing of personal data and must also apply to "data retention". Personal data must be processed on the basis of the principle of necessity to achieve the goal (need to know), not because it could potentially come in handy and make the work easier for the competent authority (nice to have). In a democratic legal state based on respect for the rights and freedoms of the individual, the legal regulation must first of all respect the privacy and freedom of the individual and only exceptionally and to the smallest possible extent can it be interfered with in certain circumstances. The reference point is thus the individual and his natural rights, not the need for public authorities to use metadata in this case. 12. I believe that the above requirements are not a self-serving limitation of law enforcement authorities in fulfilling their important role in any democratic society. The majority opinion seems to be based on the premise, already expressed by one of the interested parties - specifically the chief prosecutor Lenka Bradáčová - that due to the ever-increasing transfer of human life (and thus, among other things, crime) to the "world of data" it is necessary, for the state to have more and more powers to fight crime even in the "world of data" (at the expense of individual freedom, of course). However, I do not consider this conclusion to be inevitable. Strengthening the powers of law enforcement authorities at the expense of individual freedom is a value choice at any time and under all circumstances. It cannot therefore be argued that if more and more people live "online" and commit criminal activities there, the more powers the state must have to control these lives of ours. In the same way, it could be argued exactly the opposite, that the more our life moves into the virtual world, the more the protection of the rights of individuals and their personality and privacy should also apply to the virtual context, of which metadata is an integral part. It is this second interpretation that is more in line with how the Constitutional Court should approach the protection of human rights as the guardian of constitutionality and the fundamental rights and freedoms of the individual, and through this lens carry out a balancing act between the protection of individual rights and the public interest. 13. Although in principle I do not oppose the storage and transfer of metadata, I would like to express my disagreement with the conclusion contained in points 76, 89 and in other places, where, in my opinion, there is an impermissible simplification of the whole issue. The principle of "data retention" is accepted by the plenary with the argument of general willingness to share personal data for marketing purposes. However, this opinion ignores the fundamental difference between the voluntary sharing of data, which the data subjects can influence and which takes place for a purpose that they themselves are responsible for

achieving (receiving business offers), and which they can also terminate at any time (by withdrawing consent, leaving the social network, deleting the account , ...). On the other hand, "data retention" is the law-enforced general collection of all data (except for content), on the basis of which it is possible to create very detailed profiles of given individuals, completely independently of the will or at least the knowledge of the data subjects. Moreover, consent to the collection of this data is not given to operators by far from all their customers (see point 89 of the finding stating that it is about 70% of customers), while the Constitutional Court has the duty to protect the fundamental rights of all individuals, i.e. even those who are not willing to give their consent to the operator tracking. 14. The majority of the plenary is based on the belief that the cancellation of the contested regulation would cause a kind of chaos, less transparency, a higher risk of misuse of data, or would throw the situation into the "legislative shadow". I don't think these concerns are warranted. Revocation of the challenged legislation would of course create an urgent need to adopt a new one, however the Constitutional Court could choose, for example, a long delay in enforceability and indicate that it is not the system itself that contradicts, but only the lack of guarantees and data protection and the scope of their use. 15. Arguments about secured institutional guarantees through fines from existing bodies with a large number of other tasks or claims that no abuse of the system has been proven before the Constitutional Court do not stand either. The risk of even a high penalty has minimal deterrent potential if this risk is unlikely (after all, it is not the amount of the penalty that is important, but its inevitability). It is even more effective to set up the system in such a way that abuse cannot occur. However, the potential possibility of sanctions for possible violators of privacy beyond the legal limits and the convincing appearance of three figures from the Czech police and the public prosecutor's office during the oral hearing were enough for the majority. 16. Another important reason for greater control of data collected by private companies based on the obligations set out in the ZEK and a greater degree of prudence with their collection and use is not only the protection of individual privacy, but also the possibility of misuse outside the framework of criminal proceedings. In a similar context of social networks, it is possible to observe how individual political campaigns use data that individuals publish about themselves and that are monetized by the operators of these networks, and how this method of misuse of data collected in this way can lead to interference in the free competition of political forces. Already at the turn of the millennium, Paul Schwartz warned that the collection of personal data in cyberspace threatens not only the individual possibility of self-determination of individual people, 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 summed it up in general with the title of her paper on

privacy protection: "Where there is to be freedom, there must be privacy" (The right to privacy: Where there is to be freedom, there must be privacy. In: Šimíček, Vojtěch (ed.). Right to privacy. Brno: Masaryk University, 2011, p. 49). In a text from 2016, Boehme-Neßler warns that in the long term there will be no democracy if privacy protection is not ensured (Boehme-Neßler Volker. Privacy: a matter of democracy. Why democracy needs privacy and data protection. International Data Privacy Law . 2016, vol. 6, no. 3, pp. 222-229). 17. In conclusion, I therefore summarize that the challenged legal regulation in light of the insufficient guarantees against the misuse of collected data will not stand up, not only from the point of view of protecting the rights of individuals, but also of the entire system of our democracy. Even in comparison to other European states, our "data retention" regulation does not sufficiently protect the metadata of individuals or sufficiently control what happens to the metadata at the operator who collects it, and how it is subsequently transferred and used by the state power itself. The state, which stores and allows private companies to collect this data, does not use all options to ensure that it cannot be misused. Moreover, the legislature does not give the individual the possibility to have control over the extent to which his metadata is used by the state, and thus the individual is deprived of the possibility defend against such encroachment.