U-I-65/13-19
3 July 2014

DECISION

At a session held on 3 July 2014, in proceedings to review constitutionality initiated upon the request of the Information Commissioner, the Constitutional Court

decided as follows:

1. Articles 162, 163, 164, 165, 166, 167, 168, and 169 of the Electronic Communications Act (Official Gazette RS, Nos. 109/12 and 110/13) are abrogated.

2. Following the publication of this Decision in the Official Gazette of the Republic of Slovenia, the service providers referred to in the first paragraph of Article 163 of the Electronic Communications Act must immediately destroy all data that they are retaining on the basis of the challenged provisions.

REASONING

A

1. On the basis of the sixth indent of Article 23a of the Constitutional Court Act (Official Gazette RS, No. 64/07 – official consolidated text and 109/12 – hereinafter referred to as the CCA), the Information Commissioner submitted a request for the review of the constitutionality of Articles 162 through 169 of the Electronic Communications Act (hereinafter referred to as the ECA-1), which entered into force on 15 January 2013. By the challenged provisions, the Republic of Slovenia transposed into its legal order Directive 2006/24/EC of

the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13 April 2006 – hereinafter referred to as the Data Retention Directive).[1]

2. The applicant is the supervisory authority for supervision of the implementation of the provisions on the obligatory retention of data in conformity with the provisions of Section XIII of the ECA-1 (Article 169 of the ECA-1). It claims that it is conducting an inspection procedure with regard to the conduct of one of the Slovene mobile phone service providers, in conformity with the provisions of the ECA-1. Since in this procedure it doubted the constitutionality of the provisions on the basis of which the service provider had been retaining the traffic, location, and other therewith related data (hereinafter referred to as traffic data) of its users on the basis of the first paragraph of Article 163 of the ECA-1, the applicant submitted the request for the review of the constitutionality of the challenged provisions.

3. The fundamental allegation contained in the request for the review of the constitutionality of the challenged provisions is that, on the basis of the Data Retention Directive, the Republic of Slovenia imposed on service providers the obligation to retain as a precautionary measure data on all users, i.e. regardless of whether the users themselves gave rise to reasons for such an interference with their rights. Such retention of data allegedly entails an inadmissible interference with the right to the protection of personal data (Article 38 of the Constitution), communication privacy (Article 37 of the Constitution), and consequently also with the right to freedom of movement (Article 32 of the Constitution), the right to freedom of expression (Article 39 of the Constitution), and with the principle of the presumption of innocence (Article 27 of the Constitution). The applicant is of the opinion that, in conformity with the established constitutional case law, these measures do not pass the test of proportionality. It stresses that traffic data enjoy the same protection as the content of communications and that they are protected by Article 37 of the Constitution. It is also of the opinion that the interferences with [the mentioned human] rights are not proportionate because empirical data do not prove that the purpose of such retention of data could be achieved by such interference with the mentioned rights. Only a significantly higher percentage of serious criminal offences being investigated can allegedly justify the primacy of the public interest over the interests of every single individual with regard to enjoying privacy, moving and communicating freely (without being monitored), expressing his or her opinions, etc. The applicant is of the opinion

that the measure is not even appropriate, because there exists a series of technical circumventions that prevent the retention of data. In the opinion of the applicant, the awareness of users that their communications are being monitored also has an influence on the exercise of other rights (especially the freedom of expression). Due to self-censorship, an individual who knows that he is being monitored will act differently than he or she would otherwise. The applicant is of the opinion that due to the retention of location data, the regulation is additionally invasive, because it interferes with the freedom of movement. It also alleges a violation of Article 3a of the Constitution, which in its view lies in the fact that the Data Retention Directive has allegedly been incorrectly transposed into the Slovene legal order, because it also allows the retention of traffic data for the prevention, investigation, detection, and prosecution of criminal offences that cannot be qualified as serious criminal offences, and because it allows data to be used for the purpose of providing for the needs of the intelligence service and defence forces.

4. In its reply to the request [for the review of constitutionality], the National Assembly in fact concurs that the retention of data determined by Article 164 of the ECA-1 significantly interferes with the privacy of individuals; however, it does not concur with the standpoint of the applicant that the state does not need such data. It draws attention to the fact that the retention of data is an important tool for the detection and investigation of criminal offences, the defence of the state, national security, and constitutional regulation, and that such data must most often be obtained for a past period of time, which is precisely what the obligatory precautionary retention of data enables. The National Assembly draws attention to the provisions of the challenged regulation that reduce the possibility of abuses, namely: ten-year retention of data regarding any accessing of traffic data; service providers must retain data and protect them as confidential in conformity with the law regulating confidential data; sanctions are determined for any violation of security rules; and access to data is only possible on the basis of a court order.

5. In its opinion, the Government draws attention to the fact that the applicant, although it explicitly challenges the provisions of a national regulation, substantively alleges that the Data Retention Directive is inconsistent with the mentioned human rights. The Government does not concur with the standpoint that the retention itself of traffic data is not an important tool for the prosecution of criminal offences. It refers to the Evaluation Report on the Data Retention Directive, dated 18 April 2011,[2] from which it allegedly follows that retained traffic data such as envisaged by the Data Retention Directive have

an important role in the investigation of criminal offences. An equal conclusion allegedly also follows from the analysis with regard to the use of electronic communications traffic data for the period 2010−2012 that was prepared by the Police. From that analysis it allegedly follows that traffic data have an important role in the collection of evidence in the framework of the investigation of criminal offences, because they indicate individual facts, circumstances, relations, dynamics, and patterns that significantly contribute to the collection of fundamental evidence for directly proving the suspicion that a [concrete] criminal offence has been committed (uncovering the planning of criminal offences, the identification of persons and connections in a criminal association, etc.). The Government warns that the detection of certain criminal offences would not even be possible without the analysis of data retained beforehand (e.g. sexual abuses of children committed over the Internet). It also stresses that access to traffic data is an important tool for combating terrorism and international organised crime, as well as for the functioning of the [Slovene] Intelligence and Security Agency with the purpose of safeguarding the security of the state and its constitutional regulation. The Government explains that service providers retain traffic data in two separate databases: in the so-called "commercial" database and the "retential" database. The latter is smaller in scope, because from the "commercial" database only those data that are exhaustively determined by Article 164 of the ECA-1 are transferred thereto. Allegedly, the only consequence of the challenged regulation is a longer period of the retention of data. The Government is of the opinion that the challenged regulation does not interfere with the right to the freedom to act and the freedom of movement, and with the freedom of expression, as determined by Articles 32 and 39 of the Constitution. On the contrary, the regulation allegedly does interfere with the right to communication and information privacy determined by Articles 37 and 38 of the Constitution, as well as with the general right to privacy determined by Article 35 of the Constitution; however, these interferences are allegedly proportionate. The same allegedly applies to the alleged violation of the presumption of innocence.

6. In its reply, the applicant underlines that the allegations of the Government regarding the alleged benefits of the obligatory retention of data are generalised. It alleges that the Government does not explain what is essential: whether due to the entry into force of the obligatory retention of traffic data there was a significant change in the detection of criminal offences in comparison with the period when the regulation had not yet been in force. It is of the opinion that the analysis submitted by the Government is methodologically inappropriate and that it pursues wrong objectives. It refers

to the study of the Max Planck Institute for Foreign and International Criminal Law from 2011, from which the conclusion allegedly follows that the retention of traffic data does not contribute to a higher number of criminal offences being investigated. It also draws attention to statistical data submitted by the Government, from which it follows that only a small share of the data needed by the Police are older than 6 months. It also underlines that the perpetrators of the most serious (especially organised) criminal offences have the knowledge and means to efficiently conceal [their] electronic traces. One consequence of that is the fact that the immensely vast database containing data on the entire population will only serve to aid in the search for a handful of the most ignorant and careless perpetrators of criminal offences; for such reason, the [disputed] interferences entail a manifestly disproportionate measure.

B – I

7. The challenged provisions are contained in Section XIII of the ECA-1, entitled "Retention of data". The legislature envisaged such regulation as determined by this Section only in order to transpose into the national legal order the requirements of the Data Retention Directive.[3] In fact, the Slovene legislature first transposed the obligations stemming from the Data Retention Directive already by the adoption of the Act Amending the Electronic Communications Act (Official Gazette RS, No. 129/06 – hereinafter referred to as the ECA-A),[4] which entered into force on 27 December 2006. The regulation of the obligatory retention of data, as a consequence of the implementation of the Data Retention Directive (except for the time limit for the retention of data being shortened from two years to the now applicable 14 or 8 months),[5] has already been in force in a virtually unchanged form for more than 7 years.

8. The challenged provisions impose on service providers the obligation to retain data related to the use of certain telecommunication services (telephone services in fixed and mobile networks, Internet and e-mail access, as well as Internet phone service access). On the basis of the data that are being retained, it is possible to determine who communicated with whom, when, for how long, where, and how (Article 164 of the ECA-1 and Article 5 of the Data Retention Directive). The obligation to retain data also includes unsuccessful phone calls. The content of communications is not being retained (the third paragraph of Article 163 of the ECA-1 and the first paragraph of Article 3 of the Data Retention Directive). Data related to publicly accessible phone services

are being retained for 14 months following the day of a particular communication, whereas other data are being retained for 8 months. In exception, a longer period of retention can be determined (the fifth and sixth paragraphs of Article 163 of the ECA-1 and Articles 6 and 12 of the Data Retention Directive). At the end of the retention period, service providers must destroy the data, except those data regarding which an order for accessing the data has been issued and that have been transmitted to the competent authority (the seventh paragraph of Article 163 of the ECA-1 and Article 7 of the Data Retention Directive). What is determined (in general) is the level of protection of the retention of data and the related measures that service providers must adopt themselves or in cooperation with others. The role of the Information Commissioner is also determined; the Information Commissioner can submit preliminary opinions with regard to the general act that determines in detail the manner of the protection of the retention of data (Article 165 of the ECA-1) and supervises, with certain limitations, the implementation of the provisions of Section XIII of the ECA-1 (Article 169 of the ECA-1). Service providers must retain data (if they create or process such when providing public communications services related thereto) for the purposes of obtaining data in a public communications network determined by the law that regulates criminal procedure, for the purposes of ensuring national security and the constitutional system, and the security, political, and economic interests of the state as determined by the law that regulates the Slovene Intelligence and Security Agency, as well as the defence of the state as determined by the law that regulates the defence of the state (the first paragraph of Article 163 of the ECA-1 and in a certain part also Article 1 of the Data Retention Directive). A record of any access to data and transmission of data must be ensured for ten years (the fifth paragraph of Article 166 of the ECA-1). Service providers must not disclose to the affected persons (or third persons) the fact that any data will be or has been accessed or transmitted, nor may they disclose the court order itself (the fourth paragraph of Article 166 of the ECA-1). This Section also includes special provisions with regard to the definition of the terms that are used in this Section (Article 162 of the ECA-1), the costs of the retention of data (Article 167 of the ECA-1), and data referring to the orders for accessing and transmitting data (Article 168 of the ECA-1).

9. In fact, the applicant explicitly challenges all the provisions of Section XIII of the ECA-1, however, as is evident from the third paragraph of this reasoning, it substantively challenges only those provisions that impose on service providers the obligation to retain certain data in public communications networks (also) for the purposes and in the scope envisaged by the Data

Retention Directive. [Therefore], the Constitutional Court also carried out a review [of constitutionality] in such scope.

10. Substantively, the applicant in fact alleged that the Data Retention Directive is inconsistent with human rights. The Constitutional Court was not able to decide on the constitutionality of the challenged regulation until the Court of Justice of the European Union, which has exclusive competence to assess the validity of the mentioned Directive, decided on its validity. Therefore, by Order No. U-I-65/13, dated 26 September 2013, the Constitutional Court stayed the proceedings to review the constitutionality of the challenged provisions of the ECA-1 until the Court of Justice of the European Union adopted a decision in the joined cases Nos. C-293/12 and C-594/12, which when the Constitutional Court decided to stay the proceedings were already in the final phase of decision-making.

11. By its Judgment in the joined cases *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others* and *Kärntner Landesregierung and others*, C-293/12 and C-594/12, dated 8 April 2014 (hereinafter referred to as the Judgment in the joined cases C-293/12 and C-594/12), the Court of Justice of the European Union declared the Data Retention Directive invalid. It established that by its adoption, the legislature of the European Union exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7 and 8, as well as the first paragraph of Article 52 of the Charter of Fundamental Rights of the European Union (OJ C 326, 26 October 2012, p. 391 – hereinafter referred to as the Charter).

B – II

12. By declaring the Data Retention Directive invalid, the obligation of Member States to transpose the requirements from this Directive into the national legal order ceased. Nonetheless, the protection of traffic data still remains a subject of regulation under European Union law. Articles 5 and 6 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications) (OJ L 201, 31 July 2002) impose on Member States the obligation to ensure the confidentiality of communications and related traffic data, if they are not necessary for achieving the purpose of the transfer of communications or if an individual did not give his or her consent for such

processing of the mentioned data. Article 15 of this Directive enables that "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, […] of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

13. Therefore, European Union law does not prohibit the retention of traffic data for purposes such as are determined by the first paragraph of Article 163 of the ECA-1. Consequently, a Member State may decide to adopt such a measure. If it does, however, it must respect the requirement of the proportionality of the measure, in conformity with the limitations referred to in the mentioned provision of the Directive. From such a perspective, the Slovene legislature is entitled to determine the obligatory retention of traffic data also for the purposes of safeguarding national security, defence, and public safety, as well as [for the purposes of] preventing, investigating, detecting, and prosecuting criminal offences. In conformity with the mentioned provision of the Directive, such interference with fundamental rights must entail a necessary, appropriate, and proportionate measure within a democratic society. Also in conformity with the established constitutional case law, there has to exist a constitutionally admissible objective in order for an interference with any human right – and thus also with the right to information privacy determined by the first paragraph of Article 38 of the Constitution – to be admissible, and in addition, such interference must also be in conformity with the principles of a state governed by the rule of law, namely with that of these principles that prohibits excessive interferences by the state (the general principle of proportionality – Article 2 of the Constitution).[6] The admissibility of the limitation of the right to the protection of personal data is thus also, in conformity with the Constitution, substantively regulated in the same manner as follows from Article 15 of the mentioned Directive.

14. On the basis of the challenged regulation, as a precautionary measure service providers non-selectively retain, for a determined period of time, exhaustively determined traffic data on all communications related to fixed network phone service, mobile phone service, Internet access, Internet e-mail service, and Internet phone service. The Government alleges that these data indicate individual facts, circumstances, dynamics, and patterns of individuals' lives. With regard to the definition [of personal data] in point 1 of Article 6 of the Personal Data Protection Act (Official Gazette RS, No. 94/07 – official consolidated text – hereinafter referred to as the PDPA-1), which determines the system of protection of personal data, personal data is any data relating to an individual, irrespective of the form in which it is expressed. An individual is an identified or identifiable natural person to whom personal data relates; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, where the method of identification does not incur large costs or disproportionate effort or require a large amount of time (point 2 of Article 6 of the PDPA-1). Therefore, on the basis of the challenged regulation, service providers are retaining data that include, from the viewpoint of privacy, information regarding identifiable individuals, who must thus enjoy the protection of personal data as guaranteed by Article 38 of the Constitution. The Constitutional Court does not deal with the question of whether absolutely all traffic data that are determined by the challenged regulation are in any event personal data in the sense of the definition mentioned above.[7] What is key is that from these data (combined) it is possible to draw details from individuals' lives, and they must thus enjoy protection from the viewpoint of the right to privacy. Or, as stated by the Court of Justice of the European Union in the Judgment in the joined cases C-293/12 and C-594/12 (paragraph 27): "Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."

15. The retention of such data (also for the purposes envisaged by the challenged regulation) entails, with regard to the established constitutional case law and also the case law of the Court of Justice of the European Union,[8] an interference with the right to the protection of personal data guaranteed by Article 38 of the Constitution, Article 8 of the Charter[9], and also Article 8 of the Convention for the Protection of Human Rights and

Fundamental Freedoms (Official Gazette RS, No. 33/94, MP, No. 7/94 – hereinafter referred to as the ECHR).[10]

16. From the established constitutional case law it follows that the first paragraph of Article 38 of the Constitution guarantees the protection of personal data as a special aspect of privacy. The purpose of the protection of personal data is to ensure respect for a special aspect of human privacy – so-called information privacy. As the Constitution regulates this right specifically, it has a special place and importance in the general protection of the privacy of an individual. It also has an important place on the level of the European Union. Article 8 of the Charter also in a declaratory manner elevated the right to the protection of personal data to the level of a fundamental human right. In conformity with the established constitutional case law, any collecting and processing of personal data entails an interference with the right to the protection of privacy, i.e. with the right of individuals to keep information regarding themselves [private], because they do not want others to be acquainted therewith. The fundamental value foundation of this right is the realisation that individuals have the right to retain information regarding themselves to themselves and that as a starting point it is they who can decide how much information concerning themselves they will reveal and to whom.[11] However, the right to information privacy is not unlimited and absolute. Therefore, individuals must accept the limitations of information privacy, i.e. allow interferences therewith that are in the prevailing public interest and if the constitutionally determined conditions are fulfilled. [Such] an interference is admissible under the conditions determined by the third paragraph of Article 15 and Article 2 of the Constitution. In such context, the Constitutional Court must assess whether the legislature followed a constitutionally admissible objective, and if did, also whether the limitation is in conformity with the principles of a state governed by the rule of law, namely with that principle that prohibits excessive interferences by the state (the general principle of proportionality).[12] In the law it must be precisely determined which data may be collected and processed, and for what purpose they may be used; supervision over the collection, processing, and use of personal data must be envisaged, as well as protection of the confidentiality of the collected personal data. The purpose of the collecting of personal data must be constitutionally admissible. Only data appropriate and urgently necessary for the implementation of the statutorily defined purpose may be collected.[13] When what is at issue is the processing of personal data for the purposes of police work, the legislature must weigh the measure by which it interferes with a sensitive area of the privacy of an individual without his or her consent in an especially meticulous manner.[14] The same also applies to the

processing of personal data by other authorities of the state for the purposes of the defence of the state, national security, and the constitutional system.

17. The Constitutional Court has already explained numerous times that substantively similar requirements to those included in Article 38 of the Constitution are also included in the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Official Gazette RS, No. 11/94, MP, No. 3/94 – hereinafter referred to as the CPI). In addition to the fact that personal data must be obtained and processed fairly and lawfully, the CPI requires that measures be taken that will ensure that personal data will be retained for specified and legitimate purposes and that they will not be used in a way incompatible with those purposes, as well as that only data that are adequate, relevant, and not excessive in relation to the purposes for which they are retained will be processed (Article 5 in relation to Article 4 of the CPI).[15]

18. The first condition for the admissibility of an interference with the right determined by the first paragraph of Article 38 of the Constitution is thus the existence of a constitutionally admissible objective. The fundamental purpose of the Data Retention Directive, due to which the legislature instituted the challenged regulation, was determined by the first paragraph of Article 1 [of the Directive],[16] namely "[…] to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law." Similarly, also the first paragraph of Article 163 of the ECA-1 determines that "[service providers] must retain, for the purposes of obtaining data in a public communications network determined by the law that regulates criminal procedure, for the purposes of ensuring the national security and the constitutional system, and the security, political, and economic interests of the state, as determined by the law that regulates the Slovene Intelligence and Security Agency, as well as the defence of the state, as determined by the law that regulates the defence of the state, the data determined by Article 164 of this Act, if they create or process it when providing public communications services related thereto." The prosecution of serious forms of criminal offences, the defence of the state, and the safeguarding of the security of the state with the purpose of ensuring the protection of human rights and fundamental freedoms, as well as other fundamental legal values from illegal attacks against them are constitutionally admissible objectives. In order for the state to be able to protect human rights on its territory (Article 5 of the Constitution), it must primarily foster the existence and efficient functioning of the institutions of a state governed by the

rule of law also in such a manner that it combats the most serious forms of criminal offences, ensures the defence of the state, the national security, and the constitutional system.

19. Therefore, the legislature did have constitutionally admissible objectives for interfering with the constitutionally protected right to information privacy determined by the first paragraph of Article 38 of the Constitution. From this point of view, the interference is not inadmissible.

20. The challenged measure is also appropriate for achieving the mentioned objectives, because they can in fact be achieved by the measure. Undoubtedly, in certain situations the retention and subsequent use of traffic data can entail an appropriate means for the investigation, detection, and prosecution of serious criminal offences. The same applies to the purposes of the defence of the state and the safeguarding of the security of the state. Such proceeds from the statements of Member States, as follows from the Evaluation Report of the European Commission[17] and other documents published on its website,[18] as well as from the analysis that was submitted by the Government in the proceedings at issue. The Government alleges that these data play an important supporting role in the collection of evidence in the framework of the investigation of criminal offences, because they indicate individual facts, circumstances, relations, dynamics, and patterns that significantly contribute to the collection of fundamental evidence directly proving the suspicion that a [concrete] criminal offence has been committed. Also the Court of Justice of the European Union assessed that with regard to the increasing importance of electronic communications, the data that had to be retained on the basis of the [now] invalid Directive provided national authorities competent for criminal prosecution additional possibilities with regard to detecting serious criminal offences and that in this regard they are a valuable means for [conducting] criminal investigations.[19] Although from the materials submitted by the Government and the documents of the Commission it is not clearly evident whether what is at issue is the use of data that otherwise in the absence of obligatory retention as envisaged by the Data Retention Directive and the now challenged regulation would not be accessible to prosecuting authorities and other competent authorities of the state, it is at the same time also not possible to conclude that these data are manifestly inappropriate for achieving the [stated] objective. Likewise, it is not evident that the measure is inappropriate even if in certain instances due to technical circumvention or specific types of use of these communications services (e.g. falsifying the number calling, the use of unregistered prepaid mobile services, the use of a service for the anonymisation of traffic over the

Internet, etc.) it is possible to cover the digital traces behind the real user or achieve anonymous use of a mobile and fixed network phone service, as well as of Internet access, which is what the applicant otherwise draws attention to. A measure is inappropriate only when the means for achieving the objective does not have a sensible connection with that objective and when the stated objective cannot be achieved in any event by the [chosen] measure, not only that [it cannot be achieved] only to a certain degree.[20] However, the fact that the constitutionally admissible objective can only be achieved to a certain degree by the [chosen] measure can significantly influence the assessment of the proportionality of such measure.

21. Even if a measure is both appropriate and useful, such does not mean at the same time that it is necessary, i.e. that in order to achieve the pursued objective no [other] less invasive measures that would interfere less with the human rights of individuals are available.[21] In the framework of the test of the necessity of a measure, the Constitutional Court assesses whether an interference is at all necessary in the sense that the objective cannot be achieved without (any) interference at all or whether the objective can be achieved without the (concrete) interference that is being assessed by means of some other [interference] that would be milder in nature.[22]

22. For such reason, it is necessary to assess whether the legislature could also achieve the purpose for which such personal data was retained also in a manner that would interfere less invasively with the right determined by the first paragraph of Article 38 of the Constitution. Due to the fact that with regard to the manner and scope of the retention of data the challenged regulation is actually a transposition of the requirements from the Data Retention Directive and was thus determined in a manner such as was determined by the now no longer valid Data Retention Directive, the underlying reasons that guided the Court of Justice of the European Union in its invalidation are key also to the assessment of the challenged Act.

23. First of all, it has to be underlined that combating serious criminal offences, especially organised crime and terrorism, the defence of the state, and ensuring national security and the constitutional system, are of fundamental importance for the functioning of a state governed by the rule of law. However, such an objective, although of fundamental importance, cannot in itself justify an unlimited interference with human rights.

24. The challenged regulation provides for the precautionary (in advance) and indiscriminate retention of traffic data [generated by] certain electronic

communications. A consequence of such regulation is that service providers retain, for a determined period, the traffic data of all users of phone services in fixed and mobile networks, data on accessing the Internet and e-mail, and data on the use of phone service over an Internet protocol, such as determined by Article 164 of the ECA-1. By the precautionary and indiscriminate retention of data created daily, service providers are creating vast databases that are being retained for 14 or 8 months and from which, at any moment, very detailed conclusions can be drawn concerning facts regarding the private life of every single individual that uses these services.[23] With regard to the fact that the modern manner of communicating predominantly entails the use of the mentioned electronic communications services,[24] such a measure in fact entails a very invasive interference with the (information) privacy of the entire population, both with regard to the scope of the persons affected by the measure and with regard to the data that are being retained. The interference with the [mentioned] right is also exacerbated by the fact that by the creation of such an extensive database of personal data on the entire population, the risk that unauthorised persons will access the retained data or that the data will be used for unlawful purposes, despite the obligations imposed on service providers by, *inter alia*, Article 165 of the ECA-1, increases substantially.[25] Such a regulation substantially interferes with the human rights and fundamental freedoms of individuals also due to the fact that the affected persons are not informed of the retention and the potential subsequent use of their data, which can in the minds of these persons generate a feeling of constant surveillance.[26] Such an intangible feeling of constant surveillance can also influence the exercise of other rights, above all the right to free expression and public communication, as guaranteed by Article 39 of the Constitution and Article 11 of the Charter.[27]

25. By the nature of the matter, the precautionary and non-selective retention of data necessarily entails that it predominantly interferes with the rights of those persons who are not and will not be even indirectly connected with the purposes for which these data were primarily collected. Both the Data Retention Directive and the Slovene legislature did not limit the retention to those data that have some reasonable and objectively verifiable connection with purpose that [the legislature] intends the measure to achieve. The non-selective and precautionary retention of traffic data necessarily entails that it will interfere predominantly with the rights of that part of the population that did not give rise to any reasons for such an interference. As also the Court of Justice of the European Union stressed,[28] by the unlimited measure also data regarding communications that would otherwise have to enjoy special protection are retained. Namely, the regulation does not allow for anonymous

use of means of communication in all those instances when confidential and untraceable use of the means of communication is necessary to achieve its purpose (e.g. phone services for assistance in emotional distress). Similarly, the challenged regulation, as well as the Data Retention Directive, did not limit the retention of data to a certain period of time, geographical area, or circle of persons who might have a certain connection with the purpose pursued by the measure.[29]

26. The question regarding the length of time personal data is retained is also important for the assessment of whether the interference [at issue] is necessary to achieve a constitutionally admissible objective. The retention and processing of personal data for a longer period of time than is necessary in order to achieve the purpose does not fulfil the [criterion of] proportionality.[30] In fact, in the fifth paragraph of Article 163 of the ECA-1, the legislature envisaged a different length of time for the retention of data regarding publicly accessible phone services (14 months), on the one hand, and all other data (8 months), on the other. However, the reasons why the legislature decided [to require] retention for such duration and why it determined a different period of retention for the mentioned data are not evident from either the reply of the National Assembly nor the opinion of the Government. The analysis already mentioned above that was submitted by the Government only includes the generalised claim that if the duration of retention was shortened, "a new adaptation of investigative procedures would be necessary." With regard to the fact that different data are collected that have, by the nature of the matter, a different utility value with regard to the duration of retention, the legislature should have taken that into consideration and correspondingly differentiated the duration of retention with regard to the usefulness of the data or with regard to the persons concerned.[31] From the mentioned documentation it is also not evident why a shorter period of retention (than was, for instance, determined by certain Member States)[32] does not suffice to achieve its purpose. With regard to the measure that includes such a broad range of different data without objective criteria being determined more precisely for such retention, it is also not possible [to carry out] a subsequent test of whether the measure only refers to what is truly necessary in order to achieve its purpose. Such measure does not fulfil the criterion of necessity nor the criterion of proportionality in the narrower sense, because it is not possible to weigh whether the correspondingly longer period of retention and the degree of interference with the privacy of individuals related thereto are proportionate to ensuring public safety or some other interest pursued by such measure.

27. The now invalidated Data Retention Directive limited the purpose of such retention only to the investigation, detection, and prosecution of serious criminal offences. The challenged regulation does not include such a limitation. Also in the regulations referred to by the challenged regulation (the first paragraph of Article 163 of the ECA-1), the legislature did not limit the processing of personal data only to certain acts (serious criminal offences) for which it would assess that due to their weight the retention of data or access to these data justify the interference with the privacy of individuals.[33] Also for such reason, the measure disproportionally interferes with the right determined by the first paragraph of Article 38 of the Constitution.

28. By determining, in the first paragraph of Article 163 of the ECA-1, the obligatory retention of traffic data, the legislature substantially interfered with the right to the protection of personal data and at the same time it did not determine in detail the circumstances on the basis of which such interference would be limited to only what is truly necessary to achieve the objective. The challenged provision thereby interfered disproportionally with the right to the protection of personal data determined by the first paragraph of Article 38 of the Constitution. Consequently, the first paragraph of Article 163 of the ECA-1, which explicitly determines the obligation to retain traffic data, is unconstitutional. The other challenged provisions of Section XIII of the ECA-1 are directly connected with this provision and do not have an independent meaning. For such reason, the Constitutional Court abrogated the challenged provisions of Section XIII in their entirety (point 1 of the operative provisions).

29. Since the challenged provisions had to be abrogated already due to the inconsistency with the right to the protection of personal data determined by Article 38 of the Constitution, the Constitutional Court did not assess the other alleged unconstitutionalities.

30. In order to prevent further disproportionate interferences with the right to the protection of personal data determined by the first paragraph of Article 38 of the Constitution, the Constitutional Court determined, on the basis of the second paragraph of Article 40 of the CCA, the manner of the implementation of this Decision. On the basis of this Article, service providers that are retaining traffic data in conformity with the first paragraph of Article 163 of the ECA-1 must immediately upon the publication of this Decision in the Official Gazette of the Republic of Slovenia destroy these data (point 2 of the operative provisions).

C

31. The Constitutional Court reached this decision on the basis of Article 43 and the second paragraph of Article 40 of the CCA, composed of: Mag. Miroslav Mozetič, President, and Judges Dr. Mitja Deisinger, Dr. Dunja Jadek Pensa, Dr. Etelka Korpič – Horvat, Dr. Ernest Petrič, Jasna Pogačar, Dr. Jadranka Sovdat, and Jan Zobec. The Constitutional Court adopted the Decision unanimously.

Mag. Miroslav Mozetič
President

Notes:
[1] Such follows from the content of the statutory provisions and especially from the second paragraph of Article 2 of the ECA-1 and the purpose of the legislature expressed in the draft act (Bulletin of the National Assembly, dated 1 October 2012, EPA 667-VI).
[2] Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), dated 18 April 2011, COM (2011) 225 final.
[3] See the explanation of Section XIII of the ECA-1 (Retention of data) in the draft act (Bulletin of the National Assembly, dated 1 October 2012): "[…] From the viewpoint of the clarity of the regulation, because what is at issue is the implementation of two different directives (the Directive on Privacy and Electronic Communications and the Data Retention Directive), a new Section is introduced in the ECA-1 that only refers to the implementation of the Data Retention Directive, as was in fact already ensured by Section X of the existing ECA (i.e. 'The protection of the privacy, confidentiality, and safety of electronic communications and the retention of data regarding electronic communications traffic'). […]"
[4] See Article 92 of the ECA-A, which introduced the new Articles 107a through 107e.
[5] The fifth paragraph of Article 163 of the ECA-1.
[6] *Cf.* Decision of the Constitutional Court No. U-I-18/02, dated 24 October 2003 (Official Gazette RS, No. 108/03, and OdlUS XII, 86).
[7] See, for instance, the Opinion on the Concept of Personal Data of 2007 of the Article 29 Working Group on Data Protection.

[8] See the Judgment in the joined cases *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, C-92/09 and C-93/09, dated 9 November 2010.
[9] See the second sentence of paragraph 29 of the Judgment in the joined cases C-293/12 and C-594/12.
[10] See, in particular, the Judgments of the European Court of Human Rights (hereinafter referred to as the ECtHR) in *Leander v. Sweden*, dated 26 March 1987, *Amann v. Switzerland*, dated 16 February 2000, *Kopp v. Switzerland*, dated 25 March 1998.
[11] See paragraph 12 of the reasoning of the Decision of the Constitutional Court No. U-I-98/11, dated 26 September 2012 (Official Gazette RS, No. 79/12).
[12] *Cf.* Decision of the Constitutional Court No. U-I-18/02.
[13] As stated already in Decision No. U-I-411/06, dated 19 June 2008 (Official Gazette RS, No. 68/08, and OdlUS XVII, 43).
[14] See Decision No. U-I-312/11, dated 13 February 2014 (Official Gazette RS, No. 15/14).
[15] As stated, for instance, already in Decision No. U-I-98/11.
[16] See also the introductory statements Nos. 4, 5, 7 through 11, 21, and 22 to the Data Retention Directive.
[17] Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), dated 18 April 2011.
[18] See, e.g., *Evidence for the necessity of data retention in the EU*, accessible at: <ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf> (accessed 2 July 2014).
[19] Paragraph 49 of the reasoning of the Judgment in the joined cases C-293/12 and C-594/12.
[20] See Decision No. U-I-201/93, dated 7 March 1996 (Official Gazette RS, No. 24/96, and OdlUS V, 27). *Cf.* also with paragraph 207 of the reasoning of the Judgment of the Federal Constitutional Court of the Federal Republic of Germany No. 1 BvR 2156/08, 1 BvR 263/08, 1 BvR 586/08, dated 2 March 2010.
[21] In the framework of the assessment of the proportionality of a measure (or the necessity of a measure in a democratic society), the ECtHR underlines that the adjective "necessary" is not synonymous with "indispensable" and at the same time it also cannot be interpreted as flexibly as, for instance, the expressions "admissible", "ordinary", "useful", "reasonable", or "desirable" (the Judgment in *Handyside v. United Kingdom*, dated 7 December 1976).

[22] As stated, e.g., in Decision No. U- I-77/08, dated 8 July 2010 (Official Gazette RS, No. 61/10).
[23] See paragraph 14 of the reasoning.
[24] See paragraphs 72 and 73 of the opinion of Advocate General Pedro Cruz Villalón in the joined cases C-293/12 and C-594/12, dated 12 December 2012, and the Judgments of the ECtHR to which he refers.
[25] *Ibidem*, paragraph 75.
[26] Namely, service providers must not reveal to the persons to whom [the relevant] data refer that they were transmitted (the fourth paragraph of Article 166 of the ECA-1).
[27] As stated already in the Judgment of the Federal Constitutional Court of the Federal Republic of Germany No. 1 BvR 2156/08, 1 BvR 263/08, 1 BvR 586/08 and paragraph 37 of the reasoning of the Judgment in the joined cases C-293/12 and C-594/12.
[28] See paragraph 58 of the reasoning of the Judgment in the joined cases C-293/12 and C-594/12.
[29] *Ibidem*, paragraph 59.
[30] Decision of the Constitutional Court No. U-I-312/11, dated 13 February 2014 (Official Gazette RS, No. 15/14). See also the Judgment of the ECtHR in *S. and Marper v. United Kingdom*, dated 4 December 2008. As stated also by Article 6 of the Directive on Privacy and Electronic Communications and point e) of Article 5 of the CPI. See also paragraph 24 of the reasoning in Decision [of the Constitutional Court] No. U-I-411/06. Article 6 of the Directive on Privacy and Electronic Communications determines the principle that traffic data that is processed must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.
[31] *Cf.* with paragraphs 63 and 64 of the Judgment in the joined cases C-293/12 and C-594/12.
[32] E.g. the six-month time limit determined by the Federal Republic of Germany in the (now in fact abrogated) Article 113a of the Telecommunications Act (*Telekommunikationgesetz*).
[33] *Cf.* the first paragraph of Article 149b of the Criminal Procedure Act (Official Gazette RS, No. 32/12 – official consolidated text and 47/13 – hereinafter referred to as the CPA) and the second paragraph of Article 150 of the CPA, where the legislature determined a catalogue of criminal offences with regard to which the measures determined by the first paragraph of Article 150 of the CPA can be ordered.