REPUBLIKA SLOVENIJA
USTAVNO SODIŠČE

U-I-152/17
4 July 2019

# PARTIAL DECISION

At a session held on 4 July 2019 in proceedings to review constitutionality initiated upon the request of the Ombudsman for Human Rights, the Constitutional Court

**decided as follows:**

**1. The fourth paragraph of Article 113, point 32 of the second paragraph of Article 123, point 32 of Article 125, and the twenty-second indent of the first paragraph of Article 128 of the Police Tasks and Powers Act (Official Gazette RS, Nos. 15/13, 23/15 – corr., and 10/17) are abrogated.**

**2. The Constitutional Court will decide separately on the remaining part of the request.**

REASONING

**A**

1. The Ombudsman for Human Rights (hereinafter referred to as the applicant) required, in addition to the review of the constitutionality of paragraphs 6 and 8 of Article 112a and the third indent of the second paragraph of Article 114a of the Police Tasks and Powers Act (hereinafter referred to as the PTPA), also the review of the fourth paragraph of Article 113 of the PTPA. The latter introduced new technical means for the performance of police tasks, namely the optical recognition of licence plates.

2. According to the applicant, the mentioned statutory provision is inconsistent with the right to privacy determined by Article 35 of the Constitution and the right to the protection of personal data determined by Article 38 of the Constitution. The applicant also alleges violations of Article 32 of the Constitution, 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), and Article 2 of Protocol No. 4 to the ECHR.

3. The challenged measure is allegedly disproportionate, as it allows the mass collection of the location data of all road users, on the one hand, and only pursues the objective of combatting the theft of vehicles, on the other. The applicant opines that the subsequent seven-day period of retention of data for the purpose of combatting the theft of motor vehicles is disproportionate as well. It draws attention to the fact that the original draft of the amendment envisaged the immediate erasure of those captured licence plate data that would not be used for the performance of [police] tasks and that would not produce any matches once compared to other databases. According to the applicant, such a regulation would prevent mass surveillance. On the contrary, the regulation at issue envisages a further seven-day period of retention of all captured data, irrespective of whether there are any matches.

4. The applicant opines that such a regulation enables mass surveillance, notwithstanding the fact that the [disputed] provision prohibits the facial recognition of the passengers in vehicles. It draws attention to the fact that the preventive and non-selective retention of data inherently entails an interference predominantly with the rights of those who are not and will not even indirectly be related to the persons who are the reason that these data were collected in the first place. The challenged regulation allegedly enables mass surveillance due to the state-of-the-art technical capabilities of modern equipment for the optical recognition of licence plates, due to their affordability, and hence due to the number of police vehicles that could potentially be equipped with such technology. In this respect, the applicant also draws attention to the fact that the measure lacks sufficient safeguards. The purpose of the use [of such technology] is formulated too broadly, no judicial review is envisaged as regards access to [the collected] data, and the measure is also not limited, either geographically or in terms of a traffic area category. The applicant also draws attention to the danger of “false positive” matches and the fact that, as a general rule, individuals will not be informed of such supervision, which will likely result in road users having a feeling of constant surveillance. Subsequent retention of data allegedly also enables data mining. In this respect, the applicant also refers to the findings of the Surveillance Camera Commissioner in the United Kingdom, who in the annual report thereof for 2014 to 2015 *inter alia* drew attention to the fact that by means of the data extracted from the system for licence plate optical recognition, which are stored for the purpose of subsequent access and analysis, it is, *inter alia*, possible to follow vehicles retrospectively, to identify all vehicles at a certain place

and at a certain time, to search for connections between people, and to analyse the profile of a person once the captured licence plate information is compared to other personal data databases.

5. Allegedly, in normal circumstances, location privacy enables individuals to move around in public spaces without their location being systematically monitored and recorded. The mere fact that the regulation envisages the collection of data in public places allegedly does not affect the question of whether it entails an interference with the privacy of individuals or not. Due to the capabilities of the technical means for the optical recognition of licence plates, which is an advanced technology for recording location points, connecting them, and using these data for various other purposes, the applicant sees therein a state of increased risk of violations of human rights. Allegedly, the regulation also excessively interferes with the right to freedom of movement determined by Article 32 of the Constitution and Article 2 of Protocol No. 4 to the ECtHR. The applicant opines that such mass surveillance of movement renders free movement impossible. It also draws attention to the fact that merely the difficulties of prosecuting authorities stemming from their use of bad technical equipment cannot entail sufficient grounds for interfering with human rights.

6. The request was sent to the National Assembly, which did not submit a reply thereto. Also the Government submitted an opinion as to the allegations in the request. In its reply, for the most part, the Government summarises the legislative file as regards the Draft Act Amending the Police Tasks and Powers Act (Official Gazette RS, No. 10/17 – hereinafter referred to as the PTPA-A). The Government believes that the challenged regulation is in conformity with the Constitution. Allegedly, the regulation does not render mass surveillance possible, as it does not allow for facial recognition and because the technical means for the optical recognition of licence plates will only be installed on police vehicles, and will not be stationary or mounted on unmanned aerial vehicles. The Government also refers to the Rules on Police Powers (Official Gazette RS, Nos. 16/14 and 59/17), which expressly prohibit the use of these technical means for the general preventive surveillance of road traffic. Allegedly, it follows from the case law of the Constitutional Court that the surveillance of road traffic can also be preventive and that as such is not inconsistent with the Constitution. The Government opines that the measure at issue is comparable with the use of technical means for discovering and proving speeding at control points and exceeding the maximum average speed on road sections as determined by the third paragraph of Article 113 of the PTPA.

7. The Government refers to numerous other states where such measures are legalised, measures that prescribe the retention of data also after the initial comparison of data is finished. It alleges that, in the United Kingdom, the retention period is two years, in Denmark and in Spain it is thirty days, in Slovakia it is seven days, in Finland twenty-four hours, whereas in Germany such data are erased immediately. The reason for prescribing a seven-day period of retention of data as

determined by the twenty-second indent of the first paragraph of Article 122 of the PTPA lies in the [fact] that a request to consult the database can be [submitted] subsequently. The government does not see therein a risk of unjustified processing of personal data. Access to data will only be granted to an authorised police officer, provided that he or she is investigating a concrete criminal offence. According to the Government, the regulation indeed interferes with the right to privacy, but only with the right to privacy of those individuals who do not fulfil the conditions for using roads or for whom a search is underway. The Government draws attention to the fact that the Information Commissioner has the power to supervise the work of the Police.

8. The opinion of the Government was submitted to the applicant. In its reply, the applicant maintained that the measure is not proportionate. It believes that the Government, in its reply, failed to provide answers to its allegations and instead only explained the advantages of the use of the technology in question. The applicant stresses that it does not follow from the request, as claimed by the Government, that the mere use of technical means for the optical recognition of licence plates is in itself inconsistent with the Constitution. Only the challenged measure is allegedly inconsistent, as it includes the processing of personal data in a manner inconsistent with the Constitution. The Rules on Police Powers, to which the Government refers, indeed determines that technical means for the optical recognition of licence plates must not be used for the general preventive surveillance of road traffic, for instance such that the equipped vehicles would be positioned in a wider area on all major traffic routes. However, such a prohibition of mass surveillance, which is merely declaratory, does not fulfil the requirement that a regulation be clear and precise when the state interferes with information privacy rights. The applicant draws attention to the fact that the definition in the mentioned Rules additionally increases the lack of clarity of the regulation by introducing the term “general preventive surveillance of road traffic.” It points to the regulation in the Federal Republic of Germany, where the retention of licence plate data is not allowed, and adds that the time limit for the retention of data is not the only reason that the regulation is inconsistent with the right determined by Article 38 of the Constitution.

9. During the proceedings, the Constitutional Court *inter alia* asked the Government for an additional explanation as to the legal basis for the automated (i.e. automatic) checking of the data that the Police capture by means of the optical recognition of licence plates, and in this respect also whether the Police are already employing the optical recognition of licence plates and what the scope of such usage is. The Government stated that the Police are not yet using technical means for the optical recognition of licence plates. According to the applicant, this fact proves that the introduction of this technical means was not as urgently necessary as the Government claimed.

10. On the basis of Article 6 of the Constitutional Court Act (Official Gazette RS, No. 64/07 – official consolidated text and 109/12 – hereinafter referred to as the CCA), and in accordance with the *mutatis mutandis* application of the first paragraph of Article 314 of the Civil Procedure Act (Official Gazette RS, No. 73/07 – official consolidated text, 45/08, and 10/17), the Constitutional Court assessed that in the part that refers to the fourth paragraph of Article 113 of the PTPA, the time is ripe to decide on such request. The Constitutional Court will decide separately on the part of the request that refers to the review of the constitutionality of the first through sixth and the eighth paragraphs of Article 112a, and of the third indent of the second paragraph of Article 114a of the PTPA (Point 2 of the operative provisions).

**B – II**

**The Content of the Reviewed Regulation**

11. The fourth paragraph of Article 113 of the PTPA reads as follows: “In order to ascertain the conditions for drivers and vehicles to use roads and for searching for persons and objects, police officers may also use, in or on police vehicles, technical means for the optical recognition of licence plates. The mentioned technical means must be used in a manner that does not enable mass surveillance or facial recognition.”

12. Point 32 of Article 125 of the PTPA determines the content of the database resulting from the optical recognition of licence plates: “[...] the date, time, and location of the recording, a photograph of the licence plate, and the licence plate number.”

13. The twenty-second indent of the first paragraph of Article 128 of the PTPA determines that the data from the database resulting from the optical recognition of licence plates shall be retained for seven days.

14. In the fourth paragraph of Article 113 of the PTPA, the proposer of the PTPA-A wished to introduce a new technical means for the performance of police tasks, one intended to collect data, namely the automatic checking of licence plates or the optical recognition of licence plates.[1] The established abbreviation for this measure is ANPR (*automatic number plate recognition*).[2] This technical means functions in general in such a manner that the optical unit takes a photograph of the licence plate, the software then recognises the licence plate number, and these data are subsequently compared (cross-checked) with other personal data databases. If the data match (i.e. there is a hit), the system notifies the police officer, and on such grounds the police officer may stop the driver and the vehicle and carry out a more detailed check. Licence plate data that produce no matches are to be either

immediately deleted or further retained. The legislature chose the latter solution. From the draft act it follows that the purpose of introducing this technical means was twofold: to ensure road safety and to [facilitate] searches for persons and objects. The measure was designed with the purpose of combatting the most severe violations of road traffic regulations and for tracing stolen vehicles and [wanted] persons.[3]

15. From the legislative file it follows that there are multiple reasons for introducing the mentioned technical means. Once the highway network was built, the majority of traffic flows moved there, where ordinary preventive traffic control is rendered more difficult. The proposer of the PTPA-A also refers to the worsened traffic safety record in 2015 in comparison with the previous year. Persons without a driver's licence, unregistered vehicles, vehicles without a registration certificate, and stolen vehicles whose navigation and safety systems were interfered with allegedly pose a significant risk to the safety of road traffic. The optical recognition of licence plates allegedly entails an effective means of establishing whether the conditions for drivers and vehicles to use roads are fulfilled. According to the opinion of the Government enclosed with the draft PTPA-A, the use of this technical means will only entail an interference with the privacy of those individuals who do not fulfil the conditions for driving or who use vehicles that do not fulfil the conditions for driving, and of individuals who drive stolen vehicles, vehicles with stolen licence plates, or vehicles that authorities are searching for. The optical recognition of licence plates allegedly only entails an enhancement of police powers when controlling road traffic. Allegedly, it does not entail a new police power; instead of the hitherto manual checking of data on vehicles and drivers, the measure at issue allegedly enables the automated recognition of licence plates. According to the opinion of the Government enclosed with the draft PTPA-A, traffic control is only effective if it is preventive and based on the non-selective collection of data. The measure is based on the non-selective collection of data and on the automatic checking of the collected licence plate data in other databases.[4]

16. Four databases are listed in the legislative file,[5] (i.e. the database of registered motor vehicles and trailers, the database of issued driver's licences, the database of wanted or missing persons, and the database of lost or stolen and found objects). While the proceedings for the review of the constitutionality of the challenged provision were pending, the Government first extended the set of databases against which the data checking would be carried out to also include the database of missing persons and the database of measures ordered by courts; however, in the last clarification, dated 21 September 2018, the latter database was no longer listed.

17. In addition to [improving] road safety, the measure would allegedly render the combatting of organised crime more effective. Allegedly, due to its geographic location, the Republic of Slovenia is a transit state for organised crime, and if the

optical recognition of licence plates were introduced, it would be easier for the Police to act proactively.

18. In order to prevent the measure from entailing mass surveillance, in the draft PTPA[-A] the Government envisaged that the system for the optical recognition of licence plates would not be used in a stationary manner, but would be mounted on police vehicles, and that, when organising work, the Police would have to take into account that the measure at issue would not be used in a manner that would enable the mass surveillance of road users.[6] The initial draft act envisaged the immediate deletion of data if they do not entail a basis for a further police action, namely with a view to reducing the invasiveness of a measure that interferes with the rights of road users and to preventing mass surveillance. In such a manner, the risk of the possible unauthorised use of personal data would allegedly be avoided. However, subsequently in the legislative procedure this limitation was eliminated. Instead of the immediate deletion of data, the retention of data for seven days was enacted (the twenty-second indent of the first paragraph of Article 128 of the PTPA). The reason for introducing the seven-day period of retention of data was allegedly in particular to facilitate the investigation of thefts of motor vehicles, where information on "who drove a vehicle to the location of a theft, who carried out the theft, and who finally drove the vehicle away" is essential for successfully investigating such criminal offence.[7] In the reasoning of the amendment it is also stated that it is possible that the retention of data will also be "of essential importance in the investigation of other criminal offences, such as a bomb or terrorist threat, a murder, or manslaughter."[8]

***The Established Review of Constitutionality from the Viewpoint of Article 38 of the Constitution***

19. The first paragraph of Article 38 of the Constitution guarantees the human right to the protection of personal data. The Constitutional Court has stressed a number of times that the constitution-framers thereby specifically protected one aspect of one's privacy, namely information privacy.[9] By regulating this right independently, the Constitution confers thereon a special place and importance within the overall protection of an individual's privacy.

20. From Decision of the Constitutional Court No. U-I-98/11, dated 26 September 2012 (Official Gazette RS, No. 79/12), it follows that the fundamental value basis of this constitutional provision is the realisation that individuals have the right to keep information about themselves private and that fundamentally it is they who can decide how much of themselves they will reveal and to whom. A certain degree of concealment from the gaze of others is a necessary prerequisite to the free development of individuals and the intellectual and spiritual potential of individuals. In this sense, the protection of information privacy accelerates the free creation and transfer of thought and ideas and strengthens a pluralistic democratic society. However, due to the inclusion of individuals in society, information privacy cannot be

unlimited, i.e. absolute. Therefore, individuals must, under the constitutionally determined conditions, allow the collection and processing of personal data.[10]

21. The second paragraph of Article 38 of the Constitution determines that the collection, processing, and designated use of personal data must be determined by law. Even though this constitutional provision makes a distinction between the terms collection, use, and processing of personal data, the Constitutional Court uses the term processing of personal data as an umbrella term to designate all actions that are carried out in relation to personal data in conformity with the generally accepted terminology.[11]

22. In accordance with the established constitutional case law, any processing of personal data entails an interference with the constitutional right to the protection of personal data determined by Article 38 of the Constitution.[12] The second paragraph of Article 38 of the Constitution requires that the processing of personal data be subject to statutory regulation.[13] An interference with the right to the protection of personal data is admissible if in the law it is, *inter alia*, precisely determined which data may be collected and processed. Only data that are appropriate and necessary for the realisation of the statutorily determined purpose may be collected.[14] An interference with the constitutional guarantee of the protection of personal data is admissible in the cases referred to in the third paragraph of Article 15 of the Constitution, provided that the legislature pursued a constitutionally admissible objective and that the limitation is in conformity with the principles of a state governed by the rule of law (Article 2 of the Constitution), namely with that principle that prohibits excessive interferences by the state – i.e. the general principle of proportionality.[15]

23. The requirement that the processing of personal data must be subject to statutory regulation does not signify the mere existence of a statutory provision that enables the processing of personal data in a certain manner; instead, such a statutory provision must also be in conformity with those principles of a state governed by the rule of law determined by Article 2 of the Constitution that require that provisions be defined sufficiently clearly and precisely so that they can be implemented in practice, so that they do not allow arbitrary actions by the executive branch of power, and so that they determine with sufficient precision the legal position of the entities to which they refer. In a regulation that refers to the delicate field of information privacy with which the state interferes by collecting personal data, the requirement that provisions be sufficiently clear and precise so as to establish the meaning of the regulation holds special importance.[16]

24. Also according to the case law of the European Court of Human Rights (hereinafter referred to as the ECtHR) the requirement of the legality of an interference determined by the second paragraph of Article 8 of the ECHR *inter alia* requires that the measure be predictable in the sense that its provisions are

sufficiently detailed, clear, and precise for citizens to be able to know under which conditions and under which circumstances state authorities may carry out the measure in question, while the national law must include, in conformity with the principle of a state governed by the rule of law, appropriate and effective safeguards against arbitrary interferences and abuses.[17] Such an assessment depends on the circumstances of the case, such as the nature, scope, and duration of the measure, the conditions under which carrying out the measure is allowed, which authorities are competent to authorise, carry out, and supervise the measure, and which legal remedies are available.[18] As regards measures that entail an interference with the right to the protection of personal data, the ECtHR determined that the legal regulation thereof must *inter alia* determine clear and precise rules as to the scope and employment of the measure, as well as minimum requirements as regards the duration [of the measure], data retention, use, third party access [to the data], procedures for ensuring the completeness and confidentiality of the data, and the procedure for the destruction of the data. It is precisely in such manner that sufficient guarantees against the risk of abuse and discretion are ensured. Furthermore, such a requirement as to the quality of such a legal regulation is also tightly connected with the question of the proportionality of the measure, i.e. with an assessment of whether the measure at issue is necessary in a democratic society.[19]

***The Statutory Basis for the Automatic Checking of Data***

25. From the CPIAPPD, Directive 2016/680, and the Personal Data Protection Act (Official Gazette RS, No. 94/07 – official consolidated text – hereinafter referred to as the PDPA-1), all of which adopted a broad, all-inclusive definition, it follows that personal data are any information regarding a determined or determinable individual; a determinable individual is someone who can be determined either directly or indirectly.[20] Accordingly, the challenged regulation envisages the processing of personal data. Namely, licence plate data (together with the date, location, and time when a photograph was taken)[21] entail personal data because they refer to information regarding the vehicle of a determined or determinable individual. Since the purpose of the measure *inter alia* also includes the elimination of persons from traffic who do not fulfil the conditions to use roads and the search for persons, it is obvious that licence plate data is intended precisely to identify individuals and thus entails personal data, in conformity with the definition mentioned above.

26. As is evident from the legislative file and the explanation of the Government, the key element of the challenged measure is the automatic (i.e. automated) comparison of collected licence plate data with [data from] other personal data databases. Only on such a basis can the Police assess whether a vehicle or the driver thereof should be additionally checked. Without such a possibility, the mere collection of licence plate data is devoid of purpose. However, from the challenged provision it does not expressly follow that the collected licence plate data will be automatically compared

with other personal data databases, and even less against which personal data databases such comparison will be carried out.

27. In the proceedings [before the Constitutional Court], the Government explained that the legal basis for the automatic comparison of data is the fourth paragraph of Article 113 of the PTPA in conjunction with Articles 112 and 122 of the PTPA. Also from the legislative file it allegedly follows that the comparison of data shall be carried out automatically. The applicant did not make an express statement as regards this explanation of the Government, which was sent to the applicant for a reply thereto.

28. From the fourth paragraph of Article 113 of the PTPA it follows that the Police may use [devices for the] optical recognition of licence plates mounted on or in police vehicles, namely for the two already mentioned purposes – to ensure road safety and to [facilitate] a search for persons and objects, provided that the use of the technical means at issue will not entail mass surveillance or facial recognition. It is also determined which data will be collected in such a manner (point 32 of Article 125 of the PTPA). Such entails that the legislature did in fact enable the Police to automatically record licence plates and, consequently, to retain the data collected in such a manner in a special database for seven days (the twenty-second indent of the first paragraph of Article 128 of the PTPA). However, this provision does not in and of itself enable the Police to also carry out the next and key step in the process of personal data processing for the purposes of the envisaged measure, namely to automatically (i.e. in an automated manner) compare all these recorded and stored data with [data from] other personal data databases.

29. Article 112 of the PTPA, to which the Government refers, also does not constitute the basis for such processing of personal data. The first paragraph of this Article is merely a general provision which determines that the Police also process personal data in the performance of police tasks. The automatic (i.e. automated) personal data processing referred to in the last sentence of the first paragraph of Article 112 of the PTPA only refers to fingerprint data, palm prints, photographs, and DNA profiles.[22] The second paragraph of Article 112 of the PTPA determines that the Police may collect data directly from the person concerned or from other sources, and also from personal data databases, official databases, public records, and other databases. The other paragraphs of this provision are irrelevant as well.[23]

30. Also Article 122 of the PTPA, to which the Government refers, cannot entail a statutory basis for such processing of personal data. This provision only sets limitations as regards the automated processing of personal data for the purpose of the performance of police tasks and prohibits the creation of personal profiles merely on the basis of automated data processing.

31. Actually, the Police have a general legal basis for accessing personal data databases even when the data controller is a third party (the first paragraph of Article

115 of the PTPA). However, this provision does not regulate the processing of personal data that includes automatic (automated) access to data or the automatic comparison of data. It was conceived for dealing with individual cases.[24] The automatic comparison of data, such as envisaged by the legislature, on the other hand, entails a significantly different measure. The non-selective collection of personal data and the automatic comparison thereof with other [data from] databases by means of modern technical means for processing personal data inherently entails checking the data of a significantly broader circle of individuals. Therefore, such processing of personal data for the purpose of the performance of police tasks is, in terms of both scope and nature, incomparably different compared with that envisaged in the first paragraph of Article 115 of the PTPA.

32. The requirement of the second paragraph of Article 38 of the Constitution that the processing of personal data be subject to statutory regulation signifies that there must exist a statutory basis for every single action taken in relation to personal data, which means for every step in the process, including the collection of data, the retention thereof, access thereto, the transfer, analysis, and comparison thereof, and all other steps envisaged by the measure in question.

33. The challenged provision does not fulfil the mentioned requirements. The measure of automatic licence plate checking as envisaged by the Government in the draft PTPA-A includes, as already stated, the collection of data and then the comparison of data collected in such a manner with other personal data databases. Each of the two data processing steps entails an independent interference and requires the independent, statutorily structured, regulation of personal data processing.[25]

34. Since the challenged provision fails to determine that the collected licence plate data can be further processed by automatic (i.e. automated) comparison with other personal data databases, and the Government did not convincingly explain that other provisions of the PTPA determine such, the regulation at issue is for this reason alone inconsistent with the requirement referred to in the second paragraph of Article 38 of the Constitution. Therefore, the Constitutional Court was not in a position to assess the allegations of the applicant and to carry out a so-called strict test of proportionality, i.e. to review whether the measure is admissible under the conditions determined by the third paragraph of Article 15 of the Constitution and Article 2 of the Constitution.[26]

35. Since the challenged regulation determined by the fourth paragraph of Article 113 of the PTPA is inconsistent with the second paragraph of Article 38 of the Constitution, the Constitutional Court abrogated it. It also abrogated point 32 of the second paragraph of Article 123, point 32 of Article 125, and the twenty-second indent of the first paragraph of Article 128 of the PTPA, which are directly connected with the challenged provision and do not have meaning in and of themselves (Point 1

of the operative provisions). Since it follows from the explanation of the Government that in practice the Police do not employ the measure at issue, it was also not necessary to decide on the possible erasure of data that would be stored on the basis of an unconstitutional legal basis.[27] The Constitutional Court did not assess the other alleged unconstitutionalities because the challenged provisions had to be abrogated already due to their inconsistence with the right to the protection of personal data determined by Article 38 of the Constitution.

**C**

36. The Constitutional Court adopted this Decision on the basis of Article 43 and the first paragraph of Article 6 of the CCA, composed of: Dr Rajko Knez, President, and Judges Dr Matej Accetto, Dr Dunja Jadek Pensa, Dr.Dr. Klemen Jaklič, Dr Etelka Korpič – Horvat, Dr Marijan Pavčnik, Marko Šorli, and Dr Katja Šugman Stubbs. The Decision was adopted unanimously.

Dr Rajko Knez
President

---

[1] Government of the Republic of Slovenia, Draft Police Tasks and Powers Act – PTPA-A, dated 27 October 2016, p. 58.
[2] In the annex to the Draft PTPA, the Government termed the measure “automated number plate recognition in controlling road traffic (ANPR)." *Ibidem*, p. 57. See also L. Woods, Automated Number Plate Recognition: Data Retention and the Protection of Privacy in Public Places, Journal of Information Rights, Policy and Practice, Vol. 2, No. 1 (2017), pp. 1–21.
[3] Government of the Republic of Slovenia, Draft Police Tasks And Powers Act – PTPA-A, dated 27 October 2016, pp. 57 and 58.
[4] *Ibidem*.
[5] Annex (ANPR) to the Draft PTPA-A, p. 12.
[6] Government of the Republic of Slovenia, Draft Police Tasks and Powers Act – PTPA-A, dated 27 October 2016, p. 58.
[7] Report concerning the Draft Act Amending the Police Tasks and Powers Act, EPA 1567-VII, dated 2 February 2017.
[8] *Ibidem.*
[9] Decision of the Constitutional Court No. U-I-238/99, dated 9 November 2000 (Official Gazette RS, No. 113/2000, and OdlUS IX, 257), Para. 16 of the reasoning.
[10] Decision of the Constitutional Court No. U-I-98/11, Para. 12 of the reasoning.
[11] Decision of the Constitutional Court No. U-I-98/11, footnote 3, and Decision of the Constitutional Court No. U-I-411/06, dated 19 June 2008 (Official Gazette RS,

No. 68/08, and OdlUS XVII, 43), footnote 11. See also Article 2 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Official Gazette RS, No. 11/94, MP, No. 3/94 – hereinafter referred to as the CPIAPPD), Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4 May 2016) and Article 3 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4 May 2016 – Directive 2016/680).

[12] Decision of the Constitutional Court No. U-I-238/99, Para. 18 of the reasoning.

[13] Decisions of the Constitutional Court No. U-I-238/99, Para. 16 of the reasoning, No. U-I-92/01, dated 28 February 2002 (Official Gazette RS, No. 22/02, and OdlUS XI, 25), Para. 25 of the reasoning, No. U-I-298/04, dated 27 October 2005 (Official Gazette RS, No. 100/05, and OdlUS XIV, 77), Para. 7 of the reasoning, No. U-I-57/06, dated 29 March 2007 (Official Gazette RS, No. 33/07, and OdlUS XVI, 22), Para. 62 of the reasoning, and No. U-I-411/06, Para. 62 of the reasoning.

[14] Decisions of the Constitutional Court No. U-I-238/99, Para. 18. of the reasoning, No. U-I-411/06, Para. 19 of the reasoning, and No. U-I-312/11, dated 13 February 2014 (Official Gazette RS, No. 15/14, and OdlUS XX, 20), Para. 25 of the reasoning.

[15] Decision of the Constitutional Court No. U-I-18/02, dated 24 October 2003 (Official Gazette RS, No. 108/03, and OdlUS XII, 86), Para. 25 of the reasoning.

[16] Decision of the Constitutional Court No. U-I-411/06, Para. 60 of the reasoning.

[17] The ECtHR Judgment in *Benedik v. Slovenia*, dated 24 April 2018, Para. 122 of the reasoning (and the judgments cited therein).

[18] *Ibidem*, Para. 125 of the reasoning.

[19] The ECtHR Judgments in *S. and Marper v. the United Kingdom*, dated 4 December 2008, Para. 99 of the reasoning, and *Surikov v. Ukraine*, dated 26 January 2017, Para. 73 of the reasoning.

[20] *Cf.* point (a) of the first paragraph of Article 2 of the CPIAPPD, point 1 of Article 3 of Directive 2016/680, and point 1 of Article 6 of the PDPA-1. See also Opinion No. 4/2007 of Article 29 Working Party on the definition of the term “personal data”.

[21] Point 32 of Article 125 of the PTPA.

[22] From the Draft PTPA-A (emphases added): “It is also determined that police officers may only process data on biometric characteristics of persons in identification procedures and when uncovering and investigating criminal offences. When uncovering and investigating criminal offences, police officers may compare, provided that such is imperative and necessary, fingerprints and palm prints, photographs with photographs of other people, and DNA profiles (the processing of the mentioned data is, as a general rule, carried out in an automated manner).”

[23] The third paragraph of Article 112 of the PTPA regulates the recording and reconstruction of electronic communications in its information and telecommunication system, the fourth paragraph regulates the collection and retention of data regarding one's identity and DNA profile in the event of a police procedure due to criminal offences determined by Articles 170 through 176 of the Criminal Code (Official Gazette RS, No. 50/12 – official consolidated text, 6/16 – corr., 54/15, 38/16, and 27/17 – CrC-1) that are carried out against minors, while the fifth paragraph regulates the taking of fingerprints in the event of a police procedure due to criminal offences mentioned in the law that regulates cooperation in criminal matters with EU Member States and determines the admissibility of the execution of an arrest warrant irrespective of double criminality.

[24] See, e.g., Draft Police Tasks and Powers Act, dated 20 September 2012, EVA 2012-1711-0006, the explanation of Article 115. See also M. Nunič in: M. Nunič (Ed.), *Zakon o nalogah in pooblastilih policije (ZNPPol) s komentarjem* [Police Tasks and Powers Act (PTPA) with Commentary], p. 367, GV Založba, Ljubljana 2015.

[25] *Cf.* Judgment of the Court of Justice of the European Union 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, Paras. 32–36 of the reasoning, and also Judgments of the German Federal Constitutional Court No. 1 BvR 1299/05, dated 24 January 2012, Para. 123 of the reasoning, and 1 BvR 142/15, dated 18 December 2018, Paras. 42 *et seq*. of the reasoning.

[26] Decision of the Constitutional Court No. U-I-18/02.

[27] *Cf.* Decision of the Constitutional Court No. U-I-65/13, dated 3 July 2014 (Official Gazette RS, No. 54/14, and OdlUS XX, 27), Para. 30 of the reasoning.