Up-540/11-23
13 February 2014

DECISION

At a session held on 13 February 2014 in proceedings to decide upon the constitutional complaint of Igor Benedik, Kranj, represented by Mag. Mitja Jelenič Novak, attorney in Ljubljana, the Constitutional Court

decided as follows:

The constitutional complaint against Judgment of the Supreme Court No. I Ips 216/2010, dated 20 January 2011, in conjunction with Judgment of the Higher Court in Ljubljana No. II Kp 425/2009, dated 4 November 2009, and Judgment of the District Court in Ljubljana No. K 79/2008, dated 5 December 2008, is dismissed.

REASONING

A.

1. The complainant was found guilty of the criminal offense of the possession and distribution of pornographic material determined by the third paragraph of Article 187 of the Penal Code (Official Gazette RS, No. 95/04 – official consolidated text – hereinafter referred to as the PC) in conjunction with the first paragraph of Article 7 of the Penal Code (Official Gazette RS, No. 55/08, 66/08 – corr., 39/09, and 91/11) by the judgment of the District Court in Kranj. He was handed a suspended sentence; however, the Higher Court in Ljubljana amended the judgment with regard to the criminal sanction and pronounced a six-month prison sentence on the complainant. The Supreme Court dismissed his request for the protection of legality.

2. The complainant alleges a violation of the rights determined by Articles 37 and 38 of the Constitution, since the judgment was allegedly based on evidence obtained in violation of the right to communication privacy. He states that the Swiss law enforcement authorities conducted a systematic review of the content of communications by Razorback network users without there being a reasonable suspicion regarding any of the users or at least reasonable grounds for suspicion that they own or exchange child pornography, and that therefore an appropriate court order to obtain such data should have been issued. The complainant also alleges that

the Police obtained the data on who the user of a certain dynamic IP address was[1] first by means of a request of the Police under the third paragraph of Article 149.b of the Criminal Procedure Act (Official Gazette RS, Nos. 96/04 – official consolidated text, and 101/05 – hereinafter referred to as the CPA), and subsequently obtained the same data also on the basis of the order of the investigating judge issued under the first paragraph of Article 149.b of the CPA.[2] In the view of the complainant, a prior court order should have been issued also for these data, since such entail both personal data as well as traffic data in electronic communications networks, and in addition, an individual has a legitimate expectation of privacy with regard to a dynamic IP address.[3] The complainant alleges that the Police should have obtained a court order also for a review of the files on the computer that was seized during the house search. As the Police did not have a court order for any of the three investigative actions, the complainant states that the evidence was obtained in violation of Articles 37 and 38 of the Constitution, therefore, the judgment should not be based on this evidence and such should be removed from the file.

3. By Order of the Panel No. Up-540/11, dated 25 October 2010, the Constitutional Court accepted the constitutional complaint for consideration. Pursuant to the first paragraph of Article 56 of the Constitutional Court Act (Official Gazette RS, No. 64/07 – official consolidated text, and 109/12 – hereinafter referred to as the CCA), the Supreme Court was notified of the acceptance of the constitutional complaint.

4. On the basis of Article 5 of the CCA, the Constitutional Court requested that the office of the Information Commissioner [hereinafter referred to as the Information Commissioner], who publicly expressed its position regarding the issue of the transmission of data on subscribers of electronic communication services at the request of the Police, issue a more detailed explanation of its opinion.[4] In its comprehensive reply it explained that in its view the key issue is whether access to data on the identity of the communicating individual falls within the scope of communication privacy and is therefore regulated by the strict conditions determined by the second paragraph of Article 37 of the Constitution. It argues that law enforcement authorities do not care who the subscriber or user of a particular means of communication is, but are interested in who actually communicated with such. The reason for obtaining the identity of an individual is precisely that he communicated by means of more or less publicly accessible websites. Therefore, the Information Commissioner deems that it is necessary to change the rhetoric on the admissibility of obtaining data regarding individuals with a given IP address, be it static or dynamic, towards a a discussion of what information is actually sought. In its opinion, it is impossible to separate traffic data from subscriber data as traffic data alone does not make any sense if one does not ascertain who the person behind these data is, and the Information Commissioner deems such to be an extremely important element of communication privacy. It also opines that communication privacy entails not only the content of the communication, but also the facts and circumstances related to the communication, which also include information on who communicated when and with whom. It also highlighted that the provisions of the Electronic Communications Act (Official Gazette RS, No. 13/07 – official consolidated text, 110/09, and 33/11) in force at the time in question, which are in its opinion in accordance with the second paragraph of Article 37 of the Constitution, require a court order regarding all data related to electronic communications, irrespective whether such relates to traffic or identification data (e.g. who is using a certain IP address or telephone number). In its view, the third paragraph of Article 149.b of the CPA, which requires only a written request of the Police to obtain data on who was communicating, is constitutionally

problematic. Its criticism expressed publicly regarding the draft proposal of the seventh paragraph of Article 166 of the new Electronic Communications Act (Official Gazette RS, No. 109/12 and 110/13 – hereinafter referred to as ECA-1), which initially required only a written request of a state body for access to data on a subscriber of electronic communication services, must also be understood in this light.[5] The Information Commissioner also highlights the issue that it has not yet dealt with in its opinions, namely whether an individual who publicly discloses the content of his or her communication (e.g. an individual who expresses his or her opinion publicly to a more or less wide circle of readers on the web) continues to enjoy the protection determined by Article 37 of the Constitution regarding traffic data.

5. The opinion of the Information Commissioner was sent to the complainant, who did not respond.

6. In the framework of deciding on the constitutional complaint, the Constitutional Court inspected court file No. K 79/2008 of the District Court in Kranj.

B. – I.

7. In the constitutional complaint the complainant states that the judgment is based on evidence obtained in violation of Articles 37 and 38 of the Constitution, but the substance of his submissions claiming that the Police should have obtained a court order for all three investigative actions only refers to the violation of Article 37 of the Constitution. Based on the above, the Constitutional Court reviewed the judgment in the light of Article 37 of the Constitution.

B. – II.

Review of the objections regarding access to the complainant's IP address by the Swiss Police

8. The complainant opposes the standpoint of the Supreme Court that the dissemination of child pornography via the internet by using the eMule application (and in this way providing content to all interested parties) cannot be defined as circumstances and facts related to the private communication of a particular computer user. In the assessment of the Supreme Court, such a manner of communication, given the general accessibility of websites and the fact that the Police could check the data without special interventions in internet traffic and only on the basis of monitoring those clients that shared the controversial content, enables a practically unidentifiable number of random contacts, therefore one cannot speak of private communication protected by Article 37 of the Constitution. The complainant alleges that the information on the dynamic IP address is a *sui generis* identification datum that exists in the space between personal and traffic data and its holder legitimately expects privacy thereof, therefore it cannot be obtained without a court order. With respect to these claims, the Constitutional Court reviewed whether the stated standpoint of the Supreme Court is in accordance with Article 37 of the Constitution.

9. The component of privacy that concerns the freedom of communication is protected twice by the Constitution: in Article 35, which sets out the general rule that everyone has the right to privacy and that privacy is inviolable, and in particular in the

first paragraph of Article 37, which provides for the privacy of correspondence and other means of communication.[6] Under the latter paragraph the Constitution guarantees free and uncontrolled communication and therewith the confidentiality of relationships an individual enters into when communicating. The conditions for restrictions of the right to the privacy of correspondence and other means of communication are determined by the second paragraph of Article 37 of the Constitution, namely a restriction of the freedom of communication is admissible if: (1) it is prescribed by law, (2) it is allowed on the basis of a court order, (3) the duration of the interference is explicitly limited, and (4) if such is necessary for the institution or course of criminal proceedings or for reasons of national security.

10. In the framework of the right to respect for private and family life, the right to communication privacy is also determined by 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) in Article 8[7] and the International Covenant on Civil and Political Rights (Official Gazette SFRY, No. 7/71, and Official Gazette RS, No. 35/92, MP, No. 9/92 – hereinafter referred to as the ICCPR) in Article 17.[8] It follows from the settled caselaw of the European Court of Human Rights (hereinafter referred to as the ECtHR) that protection under Article 8 of the ECHR is afforded not only to the content of the message but also the circumstances and facts related to the communication.[9] The ECtHR dealt with the right to respect for one's private life in relation to online communication in the judgment in the case *K.U. v. Finland* from the perspective of the victim.[10] It decided that Finland did not adequately protect the right to respect for the applicant's private life as the confidentiality requirement had been given precedence over his physical and moral integrity, and consequently had violated the applicant's right determined by Article 8 of the ECHR.[11]

11. The second paragraph of Article 37 of the Constitution provides a higher level of protection than Article 8 of the ECHR as it requires a court order for any interference with the right to communication privacy.[12] The constitutional review of the case must therefore be performed on the basis of the Constitution. The right to communication privacy determined by the first paragraph of Article 37 of the Constitution primarily protects the content of the communicated message. Therefore, it ensures protection of the individual's interest that no one will gain knowledge of the content of the message transmitted through any means that enable the exchange and dissemination of such data without his or her consent, as well as the interest of individuals to decide freely to whom, to what extent, how, and under what conditions they will transmit a particular message.[13] In addition to the message content, the circumstances and facts related to the communication are also protected. In accordance with this view, in Decision No. Up-106/05, dated 2 October 2008 (Official Gazette RS, No. 100/08, and OdlUS XVII, 84) the Constitutional Court extended the protection provided by Article 37 of the Constitution also to such data regarding telephone calls that by their nature constitute an integral part of communication so that such data cannot be obtained without a court order.[14] The mentioned Decision refers otherwise to telephone communication, but the same conclusion can be applied *mutatis mutandis* to other types of communication at a distance. The crucial constitutional review test for the review of the Constitutional Court whether a particular communication is protected under Article 37 of the Constitution is the test of the legitimate expectation of privacy.[15]

12. Communication via the internet takes place, in principle, in an anonymous form, which is essential for the free development of personality, freedom of speech, and the expression of ideas, and, consequently, for the development of a free and democratic society. The privacy of communication protected by the strict conditions determined by the second paragraph of Article 37 of the Constitution is therefore a very important human right that is becoming increasingly important due to technological advances and the related growing possibilities of monitoring such. It entails individuals' legitimate expectation that the state will leave them alone also in their communication through modern communication channels and that they do not necessary have to defend themselves for what they do, say, write or think. If there is a suspicion of a criminal offense the Police must have the ability to identify the individuals who have participated in a certain communication related to an alleged criminal offense, because the perpetrators are harder to trace due to this principle of anonymity on the internet. The conditions under which the Police can carry out investigative actions and whether they need a court order, however, depend on whether such entail an interference with the right to communication privacy.

13. As was pointed out above, in addition to the content of communications, Article 37 of the Constitution also protect traffic data. Traffic data signifies any data processed for the transmission of communications in an electronic communications network or for the billing thereof.[16] Such entails that the IP address is a traffic datum. The Constitutional Court must therefore answer the question whether the complainant legitimately expected privacy regarding this datum.

14. Two factors must be weighed in relation to this review: the expectation of privacy regarding the IP address and the legitimacy of this expectation, where the latter must be of such nature that the society is willing to accept it as legitimate.[17] The complainant in the case at issue communicated with other users of the Razorback network by using the eMule application to exchange various files, including those that contained child pornography.[18] With regard to the general anonymity of internet users and also the content of the files, the Constitutional Court has no doubt that the complainant expected that his communications would remain private, and he also certainly expected that his identity would not be disclosed. The question therefore is whether such expectation of privacy was legitimate. The complainant has not established that the IP address through which he accessed the internet was hidden in any way, and thus invisible to other users, or that access to the Razorback network (and thus to the content of the files) was in any way restricted, for example by passwords or other means. Namely, that by such conduct he as a user had clearly expressed his intention that he wanted to keep his communications and identity private or that he legitimately expected privacy therewith. In other words, the subject of protection afforded by Article 37 of the Constitution is communication regarding which the individual legitimately expects privacy and makes that clear to the outside world. In contrast, in the complainant's case anyone interested in exchanging such could have accessed the contested files, and the complainant has not demonstrated that his IP address was in any way concealed or inaccessible by other users of this network. This leads to the conclusion that this entailed an open line of communication with a previously undetermined circle of strangers using the internet worldwide who have shown interest in sharing certain files, while at the same time access to the IP addresses of other users was not limited to users of this network. Therefore, in the view of the Constitutional Court, the complainant's expectation of privacy was not legitimate; that which a person knowingly exposes to the public, even if from a home computer and the shelter of his or her own home, cannot be a subject of the

protection afforded by Article 37 of the Constitution. In view of the foregoing, the contested standpoint of the Supreme Court does not raise concerns regarding constitutional law. Obtaining the data regarding the complainant's dynamic IP address does not interfere with his right to communication privacy determined by the first paragraph of Article 37 of the Constitution taking into account all the circumstances of the case, therefore a court order was not necessary to access it.[19] By his conduct the complainant himself waived his right to privacy and therefore could not have a legitimate expectation of privacy therewith.

15. As a result of the decision that the conduct of the Police did not constitute an interference with the applicant's communication privacy determined by the first paragraph of Article 37 of the Constitution, the Constitutional Court also points out that it did not need to answer the question of whether it is always necessary to assess the admissibility of interferences in communication privacy strictly according to the provisions of the Constitution and not taking into the account that the interferences were the result of the conduct of the competent authorities of other states that might be bound by different conditions as regards the protection of individual human rights.

Review of the objections regarding access to data on the user of a certain IP address

16. The complainant also challenges the standpoint of the Supreme Court that by its request to the service provider under the third paragraph of Article 149.b of the CPA the Police did not acquire traffic data, but only data regarding a particular user of a determined means of communication. In the view of the Supreme Court, it is irrelevant from this respect whether the IP address was static or dynamic, as the obtained data did not reveal anything more than what was requested, i.e. only the data regarding the user of the computer through which an individual accessed the internet. The complainant argues that the data regarding the user of a dynamic IP address is at the same time personal and traffic data, which entails that the Police can obtain it only on the basis of a court order. As the Police obtained the data regarding the user on the basis of a request, the complainant opines that the evidence was obtained in violation of Article 37 of the Constitution.

17. In the case at issue, on 7 June 2006, on the basis of the third paragraph of Article 149.b of the CPA[20], the Police sent a request to the service provider for data regarding the user to whom IP address 195.210.223.200 was assigned on 20 February 2006 at 13:28. In the response, they received data regarding the user's name, surname, and address, while the time of the communication set to the nearest second was already known.[21] Then on 14 December 2006 the Police also obtained an order issued by the investigating judge on the basis of the first paragraph 149.b of the CPA[22] and the service provider also provided the traffic data on the basis of this order.[23] The main issue for the Constitutional Court at this point is therefore whether obtaining the data regarding the identity of the user of a determined IP address falls within the framework of communication privacy.

18. In accordance with the position of the Constitutional Court in Decision No. Up-106/05, Article 37 of the Constitution also protects traffic data, i.e. data regarding, for example, who, when, with whom, and how often someone communicated. The identity of the communicating individual is one of the important aspects of communication privacy, therefore it is necessary to obtain a court order for its

disclosure in accordance with the second paragraph of Article 37 of the Constitution. Despite this standpoint, the Constitutional Court decided that the complainant's allegation of a violation of Article 37 of the Constitution is unfounded in the case at issue. By his conduct, the complainant has himself waived protection of his privacy by publicly revealing both his own IP address as well as the content of his communications, and therefore can no longer rely on it as regards the disclosure of his identity. Since by such he also waived the legitimate expectation of privacy, the data regarding the identity of the IP address user no longer enjoyed protection in terms of communication privacy, but only in terms of information privacy determined by Article 38 of the Constitution. Therefore, by obtaining the data on the name, surname, and address of the user of the dynamic IP address through which the complainant communicated the Police did not interfere with his communication privacy and therefore did not require a court order to disclose his identity.[24] In view of the foregoing, the contested position of the Supreme Court is not inconsistent with Article 37 of the Constitution, and the complainant's complaints in this part are unfounded.

Review of the objections regarding the review of the computer files found on the complainant's computer

19. The complainant's final objection refers to the issue of whether the Police should have a specific court order for the review of the computer files on the complainant's computer. In this regard, the complainant objects to the standpoint of the Supreme Court that an additional court order is not required for such review, because the Police seized the computers on the basis of a search order and the computers were first sealed and subsequently also inspected and the files were copied in the presence of the complainant.

20. In accordance with Decision of the Constitutional Court No. Up-106/05, a review of data stored on an electronic device entails an interference with an individual's communication privacy determined by Article 37 of the Constitution.[25] This entails that such data storage media cannot be reviewed without a court order.[26]

21. In the case at issue, following a motion of the Police, dated 10 January 2007, the investigating judge issued a search order for a house search of the complainant's apartment on 12 January 2007 and the search was carried out on 25 February 2007.[27] It clearly follows from the motion of the Police for the search order that the Police wanted to review in particular the hard disks of computers and any other data storage media. When deciding whether to issue the order, the investigating judge was therefore aware of the fact that during the house search the Police would seize computer equipment and that they would also review such equipment. The foregoing is also clear from the search order, from which it follows that it was issued precisely with the intent to review the data stored on the computer and other data storage media (CDs and DVDs). Such entails that the interference with communication privacy was allowed by a judge by a court order, and despite the absence of detailed statutory regulation, in accordance with the constitutional guarantees the Police also allowed the complainant to be present in both instances when his computer was reviewed. In view of the foregoing, the contested standpoint of the Supreme Court is in accordance with the requirements of the second paragraph of Article 37 of the Constitution. The search order for the house search was issued with the intent to seize and review electronic data storage media, and the complainant was present in

both instances of the review of the computers and electronic data. The Constitutional Court therefore decided that the review of the files on the complainant's computer did not violate his right to communication privacy.

22. Taking into account all the arguments, there is no violation of the right to the protection of the privacy of correspondence and other means of communication determined by Article 37 of the Constitution, therefore the Constitutional Court dismissed the constitutional complaint.

C.

23. The Constitutional Court reached this Decision on the basis of the first paragraph of Article 59 of the CCA, composed of: Mag. Miroslav Mozetič, President, and Judges Dr Mitja Deisinger, Dr Dunja Jadek Pensa, Mag. Marta Klampfer, Dr Etelka Korpič – Horvat, Dr Ernest Petrič, Jasna Pogačar, Dr Jadranka Sovdat, and Jan Zobec. The Decision was reached by seven votes against two. Judges Jadek Pensa and Sovdat voted against and submitted dissenting opinions.

Mag. Miroslav Mozetič
President

Endnotes:

[1] An IP address is a number that precisely determines a device connected to the internet (the abbreviation IP stands for Internet Protocol).

[2] At the time of obtaining the data regarding the IP address and its user (20 February 2006 and 7 June 2006) the cited Criminal Procedure Act was in force, but the wording of Article 149.b thereof remained unchanged until the Act Amending the Criminal Procedure Act (Official Gazette RS, No. 91/11) came into force.

[3] IP addresses are assigned as either a static or a dynamic address. The allocation of a static IP address entails continuous use of a single IP address, while the allocation of a dynamic address entails the random allocation of a new/different IP address upon every connection to the internet.

[4] E.g. in their Opinion on the Transmission of Data Regarding Dynamic IP Addresses to the Police, No. 0712-259/2009/2, dated 11 June 2009, and similarly also in the appeal to the deputy groups, dated 4 October 2012, available at: <https://www.ip-rs.si/novice/detajl/apel-informacijskega-pooblascenca-k-previdnosti-glede-pooblastil-za-posege-v-komunikacijsko-zasebn/?cHash=d89468d16600c1ae9be3cd80e9b23275>, and in Opinion No. 0712-1/2012/2854, dated 4 June 2013.

[5] In the procedure for adopting the new ECA-1 the wording of the seventh paragraph of Article 166 was later rejected, therefore the disputed paragraph does not exist in the current ECA-1.

[6] *Cf*. Decision of the Constitutional Court No. U-I-25/95, dated 27 November 1997 (Official Gazette RS, No. 5/98, and OdlUS VI, 158).

[7] Article 8 of the ECHR determines that: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[8] Article 17 of the ICCPR determines that: "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

(2) Everyone has the right to the protection of the law against such interference or attacks."

[9] *Cf*. judgment in the case *Malone v. The United Kingdom*, dated 2 August 1984, para. 84; the same in the judgment in the case *P.G. and J.H. v. The United Kingdom*, dated 25 September 2001, para. 42.

[10] In the cited judgment, dated 2 December 2008, the ECtHR reviewed a case where an unknown perpetrator posted an ad on an Internet dating site posing as the 12-year old applicant, announcing that he was looking for an intimate relationship with a boy of his age or older “to show him the way.” The Police requested the identity of the holder of the IP address directly from the service provider, but unsuccessfully. Subsequently, a court also refused to issue a court order since there was no explicit legal provision authorising the disclosure of the holder due to such criminal offenses. The actual perpetrator was thus never found.

[11] In the cited judgment the ECtHR emphasised that the freedom of expression and confidentiality of communications are important considerations that must be respected also on the internet, but such protection cannot be absolute. In instances such as in the case at issue, the physical and moral integrity of a minor is at stake, which requires that the state acts especially diligently and sets up a system that efficiently deters the commission of criminal offences. In the view of the ECtHR, on such occasions the freedom of expression and confidentiality of communications must yield to the prevention of crime and the protection of the rights of others.

[12] *Cf*. in detail, Decision of the Constitutional Court No. U-I-40/12, dated 11 April 2013 (Official Gazette RS, No. 39/13).

[13] Similarly, G. Klemenčič in: L. Šturm (ed.), Komentar Ustave RS – Dopolnitev komentarja – A [Commentary on the Constitution of the Republic of Slovenia, Supplement – A], Fakulteta za državne in evropske študije, Ljubljana 2011, p. 522.

[14] These are so-called traffic data, e.g. regarding the last calls made and unanswered calls evident from the phone memory.

[15] *Cf*. Decision of the Constitutional Court No. U-I-25/95.

[16] Such are, for example, data relating to the routing, duration, time or volume of messages, the protocol used, the location of the terminal equipment of the sender or the recipient, the beginning, end, and duration of a connection, and similar. *Cf*. Point 25 of Article 3 of the Electronic Communications Act (Official Gazette RS, No. 43/04), which was in force at the time the data was accessed, but the current ECA-1 defines traffic data, *mutatis mutandis*, in the same manner (Point 45 of Article 3) .

[17] *Cf*. Decision of the Constitutional Court No. Up-3381/07, dated 4 March 2010 (Official Gazette RS, No. 25/10).

[18] In criminal law theory, the term "child pornography" is gradually being abandoned and the term "child sexual abuse images or materials" is increasingly being used. However, given that the ordinary courts in these proceedings used the term "child pornography" and that the same term is used in the Penal Code, the Constitutional Court also used it in this Decision for reasons of clarity.

[19] *Cf*. also Decision of the Austrian Constitutional Court No. B 1031/11, dated 29 June 2012, in which the Court dealt with a case in which the complainant chatted in an online chat (chatroom) and one of other participants had a suspicion of a criminal offense. The other participant filed a criminal complaint with the Police and gave them the web address of the chatroom and the alias (nickname) of the complainant. The Police first obtained the data on the IP address used for the communication and subsequently the data on the user (name, surname, and address) of this IP address without a court order. The Court decided, on the basis of similar constitutional requirements as those resulting from the second paragraph of Article 37 of the Constitution, that if security authorities legally obtain the content of a message from communication available to the public or communication that is closed to the public but the content is transmitted to them by one of the participants in this communication, such communication is not a subject of protection afforded by the secrecy of communications.

[20] The third paragraph of Article 149.b of the CPA determined the following: "If there are grounds for suspicion that a criminal offense for which the perpetrator is prosecuted *ex officio* was committed or is about to be committed and it is necessary for the discovery of the offense or the perpetrator to obtain data regarding the owner or subscriber of a particular means of communication in the electronic communications traffic that are not published in directories of subscribers and regarding the period within which such means was or is in use, the Police may request in writing from the electronic communications networks service provider such data even without the consent of the individual to whom such data refer."

[21] The subscriber or the party to the contract with the service provider was the father of the complainant.

[22] The first paragraph of Article 149.b of the CPA determined the following: "If there are grounds for suspicion that a criminal offense for which the perpetrator is prosecuted *ex officio* was committed, is being committed, is about to be committed or

organised and it is necessary for the discovery of the offense or the perpetrator to obtain data regarding traffic in an electronic communications network, the investigating judge may, on the basis of a reasoned proposal of the state attorney, order that the electronic communications networks service provider provide data regarding the participants, the circumstances, and facts of electronic communications traffic, such as the following: the number or other form of identification of the users of the electronic communications service, the type, date, time, and duration of the call or other electronic communications service, the amount of data transferred, and the place from which electronic communication was carried out."

[23] The complainant's allegation that the Police obtained the same data first on the basis of their own request and subsequently also on the basis of the order of the investigating judge is therefore clearly not substantiated.

[24] The issue whether traffic data, i.e. the circumstances and facts related to communication, encompasses the name, surname, and address of the person communicating via a certain, already known IP address was dealt with also by the Austrian Constitutional Court. In the above-cited Decision No. B 1031/11, dated 29 June 2012, it held, *inter alia*, that the Police may obtain data on who the user of a specified IP address is without a court order.

[25] *Cf*. also G. Klemenčič in: L. Šturm (ed.), ibidem, p. 543.

[26] Given the rapid development of communication technologies, such are no longer just personal computers, but also a variety of electronic devices that can store data.

[27] Investigative actions were therefore carried out at a time when the CPA did not have specific provisions on the inspection of electronic devices. Articles 219a and 223a were in fact introduced in the wording of the Act only by the Act Amending the Criminal Procedure Act (Official Gazette RS, No. 77/09), which came into force 17 October 2009.