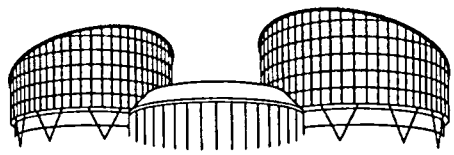

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION

CASE OF BENEDIK v. SLOVENIA

(Application no. 62357/14)

JUDGMENT

STRASBOURG

24 April 2018

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Benedik v. Slovenia,

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

Ganna Yudkivska, *President,*
Vincent A. De Gaetano,
Faris Vehabović,
Carlo Ranzoni,
Georges Ravarani,
Marko Bošnjak,
Péter Paczolay, *judges,*
and Andrea Tamietti, *Deputy Section Registrar,*

Having deliberated in private on 20 March 2018,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 62357/14) against the Republic of Slovenia lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by Igor Benedik.

2. The applicant was represented before the Court by Mr M. Jelenič Novak, a lawyer practising in Ljubljana. The Slovenian Government ("the Government") were represented by their Agent, Mrs J. Morela, State Attorney.

3. The applicant alleged, in particular, that his right under Article 8 of the Convention had been breached because the police had unlawfully obtained information leading to his identification from his Internet service provider.

4. On 8 April 2015 the application was communicated to the Government.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

5. The applicant was born in 1977 and lives in Kranj.

A. The investigation

6. In 2006 the Swiss law-enforcement authorities of the Canton of Valais conducted a monitoring exercise of users of the so-called "Razorback" network. The Swiss police established that some of the users owned and exchanged child pornography in the form of pictures or videos. Files containing illegal content were exchanged through the so-called "p2p" (peer-to-peer) file-sharing network in which each of the connected computers acted as both a client and a server. Hence, each user could access all files made available for sharing by other users of the network and download them for his or her use. Among the dynamic Internet Protocol ("IP") addresses recorded by the Swiss police was also a certain dynamic IP address, which was later linked to the applicant.

7. Based on the data obtained by the Swiss police, on 7 August 2006 the Slovenian police, without obtaining a court order, requested company S., a Slovenian Internet service provider (hereinafter "the ISP"), to disclose data regarding the user to whom the above-mentioned IP address had been assigned at 1.28 p.m. on 20 February 2006. The police based their request on section 149b(3) of the Criminal Procedure Act (hereinafter "the CPA", see paragraph 36 below), which required the operators of electronic communication networks to disclose to the police information on the owners or users of certain means of electronic communication whose details were not available in the relevant directory. In response, on 10 August 2006 the ISP gave the police the name and address of the applicant's father, who was a subscriber to the Internet service relating to the respective IP address.

8. On 12 December 2006 the police proposed that the Kranj District State Prosecutor's Office request the investigating judge of the Kranj District Court to issue an order demanding that the ISP disclose both the personal data of the subscriber and traffic data linked to the IP address in question. On 14 December 2006 such a court order was obtained on the basis of section 149b(1) of the CPA and the ISP gave the police the required data.

9. On 12 January 2007 the investigating judge of the Kranj District Court issued an order to carry out a house search of the applicant's family home. The order indicated the applicant's father as the suspect. During the house search the police and the investigating judge of the Kranj District Court seized four computers and later made copies of their hard disks.

10. Based on a conversation with the applicant's family members, of which no record is available, the police changed the suspect to the applicant.

11. Reviewing the hard disks, the police found that one of them contained files with pornographic material involving minors. The police established that the applicant had installed eMule, a file-sharing program, on one of the computers by means of which he had been able to download different files from other users of the program and had also automatically

offered and distributed his own files to them. Among the files downloaded by the applicant, a small percentage had contained child pornography.

12. On 26 November 2007 the Kranj District prosecutor requested that a judicial investigation be opened against the applicant.

13. In his defence before the investigating judge, the applicant argued, *inter alia,* that he had not been aware of the content of the files in question. He also argued that the ISP had unlawfully, without a judicial warrant, passed his data, including his address, to the police.

14. On 5 March 2008 the investigating judge of the Kranj District Court, opened a judicial investigation against the applicant on the basis of a reasonable suspicion that he had committed the criminal offence of displaying, manufacturing, possessing and distributing pornographic material under section 187(3) of the Criminal Code. The judge noted, among other things, that the applicant's father had been the holder of the identified IP address and that the applicant had allegedly been logging into the respective program under the name of "Benet".

15. On 17 March 2008 the applicant's counsel lodged an appeal against the decision to open a judicial investigation. He argued, *inter alia*, that the evidence concerning the identity of the user of the respective IP address had been obtained unlawfully. That information concerned the traffic data and should therefore not have been obtained without a judicial warrant.

16. On 21 March 2008 an interlocutory panel of the court rejected the appeal finding that, although counsel had argued that the identity of the user of the IP address had been obtained unlawfully, he had not requested that certain documents be excluded from the file.

B. The trial

17. On 29 May 2008, the Kranj District State Prosecutor's Office lodged an indictment against the applicant for the above-mentioned criminal offence.

18. At the hearing of 8 October 2008 the applicant lodged a written request for exclusion of evidence obtained unlawfully, including the information concerning the user of the respective IP address obtained without a court order.

19. On 5 December 2008 the court rejected the applicant's request, finding that the data concerning the user of the respective IP address had been obtained in compliance with section 149b(3) of the CPA.

20. On 5 December 2008 the Kranj District Court found the applicant guilty of the criminal offence with which he had been charged. Based on the opinion of an expert in computer science, the District Court held that the applicant must have been aware of the 630 pornographic pictures and 199 videos involving minors which he had downloaded through p2p networks and made available for sharing with other users. The applicant was

sentenced to a suspended prison term of eight months with a probation period of two years.

C. Proceedings before the Ljubljana Higher Court

21. Both the applicant and the district state prosecutor appealed against the first-instance judgment. The applicant challenged the facts as established by the District Court. He also alleged that the subscriber information the Slovenian police had acquired without a court order, and thus unlawfully, should have been excluded as evidence. Consequently, all the evidence based on such unlawfully acquired data should also have been excluded.

22. On 4 November 2009 the Ljubljana Higher Court granted the appeal of the district state prosecutor in part, converting the applicant's suspended sentence into a prison term of six months. The applicant's appeal was dismissed as unfounded. The Higher Court confirmed that the first-instance court had correctly established the facts of the case; moreover, it held that the data concerning the user of the IP address had been obtained lawfully, as no court order was required for such a purpose.

D. Proceedings before the Supreme Court

23. The applicant lodged an appeal on points of law before the Supreme Court, reiterating that a dynamic IP address could not be compared to a telephone number which was not entered in a telephone directory, as a new IP address was assigned to a computer each time the user logged on. Accordingly, such data should be considered as traffic data constituting circumstances and facts connected to the electronic communication and attracting the protection of privacy of communication. The applicant argued that the Swiss police should not have obtained the respective dynamic IP address without a court order, and nor should the Slovenian police have obtained the data on the identity of the subscriber associated with the IP address without such an order.

24. On 20 January 2011 the Supreme Court dismissed the applicant's appeal on points of law, reasoning that given the general accessibility of websites and the fact that the Swiss police could check the exchanges in the p2p network simply by monitoring the users sharing certain contents, that is without any particular intervention in internet traffic, such communication could not be considered private and thus protected by Article 37 of the Constitution. Moreover, in the Supreme Court's view, the Slovenian police had not acquired traffic data about the applicant's electronic communication, but only data regarding the user of a particular computer through which the Internet had been accessed.

E. Proceedings before the Constitutional Court

25. The applicant lodged a constitutional complaint before the Constitutional Court, reiterating the complaints adduced before the lower courts.

26. The Constitutional Court asked the Information Commissioner to express her position on the issue. The Information Commissioner was of the view that the reason for obtaining the identity of an individual user of electronic communication was precisely that he or she communicated by means of more or less publicly accessible websites. In the Information Commissioner's view, it was impossible to separate traffic data from subscriber data, as traffic data alone did not make any sense if one did not ascertain who the person behind those data was – this latter information was thus considered to be an extremely important element of communication privacy. The Information Commissioner also highlighted that the provisions of the Electronic Communications Act in force at the material time required a court order regarding all data related to electronic communications, irrespective of whether they related to traffic or identification data. In the Information Commissioner's view, section 149b (3) of the CPA, which required only a written request from the police to obtain data on who was communicating, was constitutionally problematic.

27. On 13 February 2014 the Constitutional Court dismissed the applicant's complaint, holding that his constitutional rights had not been violated. The Constitutional Court's decision was adopted by seven votes to two. Judge J. Sovdat and Judge D. Jadek Pensa wrote dissenting opinions. The decision was served on the applicant on 11 March 2014.

1. The Constitutional Court's decision

28. The Constitutional Court pointed out, at the outset, that in addition to the content of communications, Article 37 of the Constitution also protected traffic data, that is any data processed for the transmission of communications in an electronic communications network. It considered that IP addresses were included in such traffic data. The Constitutional Court, however, concluded that the applicant, who had not hidden in any way the IP address through which he had accessed the Internet, had consciously exposed himself to the public and could not legitimately have expected privacy. As a result, the data concerning the identity of the user of the IP address were not protected as communication privacy under Article 37 of the Constitution, but only as information privacy under Article 38 of the Constitution, and no court order was required in order to disclose them in the applicant's case.

29. The most relevant parts of the Constitutional Court's decision are as follows (as translated into English on the Constitutional Court's website):

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

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 ... The right to communication privacy determined by the first paragraph of Article 37 of the Constitution primarily protects the content of the communicated message. ... 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. 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.

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. 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 protects traffic data. Traffic data signifies any data processed for the transmission of communications in an electronic communications network or for the billing thereof. 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. 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. 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. ... In contrast, in the complainant's case anyone interested in exchanging such data 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. By his conduct the complainant himself waived his right to privacy and therefore could not have a legitimate expectation of privacy therewith.

...

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 ...

17. In the case at issue, on 7 June 2006, on the basis of the third paragraph of Article 149.b of the CPA, 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. 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 and the service provider also provided the traffic data on the basis of this order. 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. 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."

2. Dissenting opinion by Judge J. Sovdat

30. Judge J. Sovdat welcomed the Constitutional Court's departure from the Supreme Court's view that the information concerned had not amounted to traffic data. However, in her view, the police wishing to obtain identification of the subscriber should have requested a court order. She pointed out that the Constitutional Court's conclusion implied that the protection of privacy of traffic data was always dependent on the protection of the content of communication. Accordingly, traffic data concerning certain communication were protected as long as the content of that communication was protected. Consequently, an individual could not enjoy separate and independent protection of traffic data. Judge Sovdat disagreed with this view, pointing out that the applicant had not appeared in public under his own name, but only through the digits of his dynamic IP address.

31. Judge Sovdat agreed with the Information Commissioner that the police had been interested not in the ownership of the device but in "the identity of the person communicating and precisely because he had been communicating". She endorsed the Commissioner's view that "the content of communication alone did not have any particular weight in the absence of identification of those communicating". She also pointed out that under sections 166 and 168 of the new Electronic Communications Act ("ECA-1", see paragraph 39 below), the Internet provider was not allowed to transfer the stored information without a court order. Compared with section 149b(3) of the CPA, the ECA was definitely more recent and therefore the decision of the majority ran contrary to the level of rights protection already achieved.

3. Dissenting opinion by Judge D. Jadek Pensa

32. Judge D. Jadek Pensa argued that the constitutional guarantees set out in Article 37 of the Constitution were aimed at strengthening the expectation of privacy in this area of life and preventing disproportionate interferences and an abuse of power by the executive.

33. As regards the applicant's expectation of online anonymity, Judge Jadek Pensa argued that none of the data publicly disclosed by the complainant revealed his identity. In her view, anonymity was what prevented the police from linking a particular communication with a particular person – that is, linking a dynamic IP address and an individual

with his or her name and address. She further argued that the question whether the applicant's manner of communication could lead to the conclusion that his expectation of privacy had not been objectively justified had to be approached by taking all the circumstances into account, including the law that had been in force at the relevant time. She explained that the ECA (sections 103(1(2)), 104(1) and 107 – see paragraphs 37 below) required Internet providers to delete traffic data as soon as they were no longer needed for the transfer of messages. Moreover, section 107 of the ECA provided that the secrecy of communication could be interfered with only on the basis of a decision by a competent authority. A letter from the police to an Internet provider could not be considered to amount to such a decision. Thus, even if section 149b(3) of the CPA could be interpreted as allowing the police to ask for information on an Internet subscriber, it should not apply in the situations covered by the ECA, which explicitly concerned the "protection of secrecy and confidentiality of electronic communications". Otherwise, the legislation would be contradictory. The judge concluded that the applicable legal framework could not therefore have led to the conclusion that the applicant, as a reasonably and sufficiently informed individual, could not have expected privacy; that is, he could not have expected that his anonymity would be protected.

34. Judge Jadek Pensa went on to elaborate on the neutrality of traffic data, such as data on the user of a certain dynamic IP address:

> "9. The traffic datum – the dynamic IP address that was assigned randomly at a given moment – as I understand it, reveals how the internet was used on some computer, because it is inextricably attached to a specific connection. ... This is because only the two data jointly communicate how the internet was used in a non-anonymised way, i.e. regarding internet use in connection with an identified person. This essential circumstance in my opinion negates the notion of the neutrality of the datum regarding a specific user of services for a certain (known) dynamic IP address that the police sought through the service provider - namely, the neutrality of the datum in terms of denying its ability to communicate anything more than the name and address of a certain person (who has a subscription contract with the service provider). Precisely because this datum is inseparably linked to a specific communication, the traffic datum falls within the scope of protected communication privacy.
>
> 10. Even if the service provider communicated to the police 'only' the data identifying a person who had a subscription contract with it, by doing so, as I understand it, the service provider in fact communicated (to put it simply) traffic data in an electronic communications network regarding this person. The police also, as I have already explained, wanted to determine more than just the name and surname of a certain person who had concluded a contract. Since, as I understand it, they asked for traffic data associated with a particular person they would have to proceed according to the first paragraph of Article 149.b of the CPA and obtain an order from the investigating judge."

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. The Constitution

35. Articles 37 and 38 of the Constitution, which provide for the protection of privacy of correspondence and other means of communication and the protection of personal data, respectively, provide as follows:

Article 37

"The privacy of correspondence and other means of communication shall be guaranteed.

Only a law may prescribe that on the basis of a court order the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time where such is necessary for the institution or course of criminal proceedings or for reasons of national security."

Article 38

"The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.

The collection, processing, designated use, supervision, and protection of the confidentiality of personal data shall be provided for by law.

Everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data."

B. Criminal Procedure Act

36. Section 149b of the Criminal Procedure Act (Official Gazette no. 8/06), in the chapter regulating measures taken by the police in pre-trial proceedings, provided:

"(1) If there are grounds for suspecting that a criminal offence for which a perpetrator is prosecuted *ex officio* has been committed, is being committed or is being prepared or organised, and information on communications using electronic communications networks needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the investigating judge may, at the request of the public prosecutor adducing reasonable grounds, order the operator of the electronic communications network to furnish him with information on the participants and the circumstances and facts of electronic communications, such as: the number or other form of identification of users of electronic communications services; the type, date, time and duration of the call or other form of electronic communications service; the quantity of data transmitted; and the place where the electronic communications service was performed.

(2) The request and order must be in written form and must contain information that allows the means of electronic communication to be identified, an indication of reasonable grounds, the time period for which the information is required and other important circumstances that dictate use of the measure.

(3) If there are grounds for suspecting that a criminal offence for which a perpetrator is prosecuted *ex officio* has been committed or is being prepared, and information on the owner or user of a certain means of electronic communication whose details are not available in the relevant directory, as well as information on the time that the means of communication was or is in use, needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the police may request that the operator of the electronic communications network furnish them with this information, at their written request and even without the consent of the individual to whom the information refers.

(4) The operator of electronic communications networks may not disclose to its clients or a third party the fact that it has given certain information to an investigating judge (first paragraph of this section) or the police (preceding paragraph), or that it intends to do so."

C. Electronic Communications Act

37. At the time the data in question were obtained (August 2006), the Electronic Communications Act ("ECA", Official Gazette nos. 43/04 and 86/04) was in force. This Act implemented, among other things, Directive 2002/58/EC (see paragraph 56 below). The following provisions were relevant:

Section 1

Content of the Act

"This Act regulates the conditions for the provision of electronic communication networks and for the provision of electronic communication services ... determines the rights of users ... regulates the protection of the secrecy and confidentiality of electronic communications and regulates other questions related to electronic communications."

Section 3

Terms used

"The terms used in this Act have the following meaning:

...

25. Traffic data are any data processed for the purpose of the conveyance of communication on an electronic communications network or for the billing thereof.

..."

Section 103

Confidentiality of communications

"(1) Confidentiality of communications refers to:

1. the content of communications;

2. traffic data and location data connected to the communication mentioned in subsection (1)1 above;

3. facts and circumstances relating to unsuccessful attempts to establish connections.

(2) An operator and anyone involved in the provision and performance of its activities must continue to safeguard the confidentiality of communications after ceasing performance of the activity for which it was bound to safeguard confidentiality.

(3) Those entities liable under subsection (2) above may only obtain the information on communications referred to in subsection (1) above to the extent necessary for the provision of specific publicly available communications services, and may only use or transfer [*posreduje*] this information to others in order to provide these services.

(4) Where operators obtain information on the content of communications or record or retain communications and the traffic data related to them under subsection (3) above, they must notify the user of this when the subscriber contract is signed or upon the commencement of provision of the publicly available communications service, and erase information on the content of communications or the communications themselves as soon as this is technically feasible and the information is no longer necessary for the provision of the particular publicly available communications service.

(5) All forms of surveillance or interception, such as listening, tapping, recording, retention and transfer [*posredovanje*] of the communications referred to in subsection (1) above shall be prohibited, unless this is permitted under subsection (4) above or under section 107 of this Act, or if this form of surveillance or interception is necessary for the sending of messages (e.g. facsimile messages, electronic mail, electronic mailboxes, voicemail and SMS services).

..."

Section 104

Traffic data

"(1) Traffic data relating to subscribers and users, and processed and stored by the operator, should be deleted or rendered anonymous, as soon as they are no longer needed for the transfer of messages.

(2) Without prejudice to the provision of subsection (1) above, an operator may, until complete payment for a service but no longer than until the expiry of the limitation period, retain and process traffic data required for the purposes of calculation and of payment relating to interconnection.

(3) For the purpose of marketing electronic communications services or for the provision of value-added services, the provider of a publicly available electronic communications service may process the data referred to in subsection (1) above to the extent and for the duration necessary for such services or marketing, but only if the subscriber or user to whom the data relate has given his prior consent. Subscribers or users must be informed, prior to giving consent, of the types of traffic data which are processed and the duration of such processing. A user or subscriber shall have the right to withdraw his or her consent at any time.

(4) For the purposes referred to in subsection (2) above, a service provider must indicate in the general terms and conditions which traffic data will be retained and processed, and the duration thereof, and declare that they will be treated in accordance with the law on data protection.

(5) Traffic data may only be processed under subsections (1) to (4) above by persons acting under the authority of an operator and handling billing or traffic management, responding to customer enquiries, detecting fraud, marketing electronic communications services or providing a value-added service, and this processing must be limited to what is necessary for the purposes of such activities.

(6) Without prejudice to the provisions of subsections (1), (2), (3) and (5) above, an operator shall, upon a written request of a competent body set up for the purpose of settling disputes, in particular interconnection or billing disputes, and in accordance with the applicable legislation, send traffic data to such body."

Section 107

Lawful interception of communications

"... (2) An operator should enable the lawful interception of communications at a determined point of the public communication network as soon as it receives a copy of the operative part of the order of the competent authority indicating the point ... at which a lawful interception of communications should take place and other data related to the means, scope and duration of this measure."

38. Further amendments to the ECA, namely ECA-A, which were enacted on 28 November 2006, that is after the contested measures had been taken in the present case (Official Gazette no. 129/06), regulated the retention of traffic data for the purposes of, *inter alia*, criminal proceedings. This included data necessary for the identification of the source of communication, such as the name and address of the subscriber to whom a certain IP address was assigned, data needed for the identification of the destination of communications, and data needed to identify the date, time and duration of communications (sections 107.a and 107.b). No distinction between the static and the dynamic IP address was made in this regard. Furthermore, the amendment, introduced by section 107.č, stipulated that the operator was under an obligation to allow access to or to transfer the retained data immediately and no later than three days after receiving the transcript of the "order" issued by the "competent body". Section 107.e of the amended Act provided that "the court that has ordered that certain data be accessed should keep a record of data concerning orders for access and transfer of the retained data". It also regulated the reporting procedure on access to retained data – from the courts to the Ministry of Justice and then from the ministry to the European Commission.

39. On 20 December 2012 a new Electronic Communications Act ("ECA-1", Official Gazette 109/2012) was adopted. Its sections 166 and 168 provide as follows:

Section 166

Transfer of retained data to competent bodies

"(1) An operator must, immediately or without undue delay, transfer retained data as soon as it receives a copy of the operative part of an order from a competent body stating all the required data on the scope of access.

...

(4) An operator may not disclose an order to the persons to whom the order ... relates or to third parties, nor disclose that it has transferred or will transfer retained data to the competent body under this section.

...

(7) The information commissioner shall monitor the fulfilment of the obligations by the providers under this section, in so far as they do not fall under the supervision of other competent bodies on the basis of other laws."

Section 168

Data on access orders and data transfers

"(1) A court that has ordered access to data shall keep a record of access orders and the transfers of data retained pursuant to section 166 of this Act, comprising:

1. the number of cases in which access to retained data was ordered;

2. a statement of the date or period for which the data was requested, the date on which the competent body issued the data access order and the date of the transfer of the data;

3. the number of cases in which data access orders could not be executed.

(2) The competent court shall forward the record referred to in subsection (1) above for the current year to the ministry responsible for justice by no later than 31 January the following year.

(3) The ministry responsible for justice shall, on the basis of the records received from all courts, prepare a joint report on access to retained data by no later than 20 February each year for the previous year. It shall forward it to the ministry, which shall in turn forward it without delay to the European Commission and to the National Assembly Committee responsible for supervising the intelligence and security services.

(4) The ministry responsible for justice shall, after obtaining the prior opinion of the President of the Supreme Court of the Republic of Slovenia, issue instructions using the reporting forms under this section."

D. Personal Data Protection Act

40. Further to Slovenia becoming a member of the European Union, the Slovenian Parliament adopted, on 15 July 2004, a new Personal Data Protection Act (Official Gazette no. 86/04), underpinned by Directive 95/46/ES (see paragraph 53 below). It provides, in so far as relevant, as follows:

Section 1

Contents of the Act

"This Act determines the rights, responsibilities, principles and measures to prevent unconstitutional, unlawful and unjustified encroachments on the privacy and dignity of an individual (hereinafter: individual) in the processing of personal data."

Section 6

Meaning of terms

"The terms used in this Act shall have the following meanings:

1. Personal data - are any data relating to an individual, irrespective of the form in which they are expressed.

2. Individual - is an identified or identifiable natural person to whom personal data relate; 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 significant costs or a disproportionate effort or require a large amount of time.

...

18. Anonymising - is an alteration to the form of personal data such that they can no longer be linked to the individual or where such link can only be made with disproportionate efforts, expense or use of time.

19. Sensitive personal data - are data on racial, national or ethnic origin, political, religious or philosophical beliefs, trade-union membership, health status, sexual life, ..."

41. Section 2 of the Personal Data Protection Act provided that personal data should be processed lawfully and fairly. Section 8 provided that personal data could be processed if the law provided for doing so or on the basis of the consent of the individual affected. Under section 12, personal data could be processed without any other legal basis if this was urgently necessary for the protection of a person's life or limb.

42. The Personal Data Protection Act also provided that data could be collected only for defined and lawful purposes and processed accordingly (section 16) and only on condition that this was necessary for the achievement of those purposes (section 21). Thereafter they should be deleted, destroyed, blocked or anonymised (ibid). The Act also set out the measures and procedures that should be taken by operators and contracted processors to secure personal data, and to prevent accidental or deliberate unauthorised destruction of data, their alteration, loss or unauthorised processing (sections 24 and 25).

E. Criminal Code

43. The Criminal Code applicable at the material time prohibited, in its Article 187, the presentation of pornographic material to minors under the age of fourteen and the manufacturing and distributing of pornographic material depicting minors. The relevant provision reads as follows:

"...

(2) Whosoever abuses a minor for the manufacturing of pornographic pictures, audio-visual or other objects of pornographic content, or uses a minor to act in a

pornographic performance, shall be sentenced to a term of imprisonment of between six months and five years.

(3) Whosoever produces, distributes, sells, imports or exports pornographic or other sexual material depicting minors, supplies it in any other way, or possesses such material with the intent of producing, distributing, selling, importing, exporting or offering it in any other way, shall be liable to the same sentence as in subsection (2) above.

..."

F. Constitutional Court decision no. Up-106/05 of 2 October 2008

44. Case no. Up-106/05 concerned a complainant who had been convicted of the illicit manufacture and trade in narcotics, based on data (a list of telephone numbers and text messages) obtained from his SIM card, without a court order. He complained that his conviction had been based on unlawfully obtained evidence, as the police had monitored his mobile telephone communication without a court order. The Constitutional Court upheld the complaint and quashed the lower courts' judgments.

45. The Constitutional Court found that not only the content of the communication but also the circumstances and facts connected to the communication were protected, including the data stored in the telephone's memory, which were an integral element of communication privacy. Therefore, obtaining data on the last dialled and last unanswered calls entailed an examination of the content and circumstances of the communication, and were consequently an interference with the right determined in the first paragraph of Article 37 of the Constitution. The court pointed out that such interference was, pursuant to Article 37 § 2 of the Constitution, admissible if the following conditions were met: (1) the interference was prescribed by law; (2) the interference was allowed on the basis of a court order; (3) the duration of the interference was precisely determined; and (4) the interference was necessary for the institution or course of criminal proceedings or for reasons of national security.

III. RELEVANT INTERNATIONAL LAW

A. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

46. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature on 28 January 1981, ETS No. 108, hereinafter "the 1981 Convention") was ratified by all Council of Europe Member States and entered into force with respect to Slovenia on 1 September 1994. Article 1 sets out the object and purpose of the Convention, which is "to secure in the territory of each Party for every

individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')." The 1981 Convention, among other things, protects individuals against abuses and applies to all data processing carried out by both the private and public sector, such as data processing by the judiciary and law-enforcement authorities. In Article 2 "personal data" are defined as any information relating to an identified or identifiable individual. Article 5 requires that personal data undergoing automatic processing be obtained and processed fairly and lawfully.

B. Convention on Cybercrime

47. The Convention on Cybercrime (opened for signature on 23 November 2001, came into force on 1 July 2004, ETS No. 185, hereinafter "the Cybercrime Convention") took effect in Slovenia on 1 January 2005.

48. The Cybercrime Convention is the first international treaty on crimes committed via the Internet and is open to all States. It requires countries to establish as criminal offences, among others, child pornography.

49. Article 1 defines, for the purposes of the Cybercrime Convention, "traffic data" as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service." Its Explanatory Report further provides, in the relevant part, as follows (§ 30):

> "The 'origin' refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. The 'destination' refers to a comparable indication of a communications facility to which communications are transmitted. The term 'type of underlying service' refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging."

50. Pursuant to the Cybercrime Convention the following measures should be available to the authorities to combat the crimes listed therein:

> **Article 18 – Production order**
>
> "1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
>
> ...
>
> b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, the term 'subscriber information' means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a) the type of communication service used, the technical provisions taken thereto and the period of service;

b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement."

Article 20 – Real-time collection of traffic data

"1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and

b) compel a service provider, within its existing technical capability:

(i) to collect or record through the application of technical means on the territory of that Party; or

(ii) to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

...

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15."

Article 21 – Interception of content data

"1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and

b) compel a service provider, within its existing technical capability:

(i) to collect or record through the application of technical means on the territory of that Party, or

(ii) to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

...

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15."

51. With regard to the production order, the Explanatory Report to the Convention on Cybercrime (Budapest, 23 November 2001, ETS No. 185) states that, in the course of a criminal investigation, subscriber information may be needed mainly in two situations. Firstly, to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used, the type of other associated services used (for example, call forwarding, voicemail), or the telephone number or other technical address (for example, the email address). Secondly, where a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. According to the explanatory report, a production order provides a less intrusive and less onerous measure which law-enforcement authorities can apply instead of measures such as interception of content data and real-time collection of traffic data, which must or can be limited only to serious offences.

52. The Cybercrime Convention requires that the aforementioned measures provided for in Articles 18, 20 and 21 be subject to the conditions set out in Articles 14 and 15, which, as far as relevant, read as follows:

Article 14 – Scope of procedural provisions

"1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

..."

Article 15 – Conditions and safeguards

"1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure."

IV. RELEVANT EUROPEAN UNION LAW

A. Directive 95/46/EC and Regulation (EU) 2016/679

53. Article 2 (1) (a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31, hereinafter "the Data Protection Directive") provides that "personal data" means "any information relating to an identified or identifiable natural person ('data subject')". Furthermore, under the aforementioned provision, an "identifiable 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". The Data Protection Directive does not apply to the area of police and criminal justice.

54. Recital 26 provides that in determining whether a person is identifiable, "account should be taken of all the means likely reasonably to be used ... to identify the said person"; the principles of protection will not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

55. 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 2016 L 119/1, p. 1), entered into force on 24 May 2016. When it takes effect (25 May 2018), it will replace the Data Protection Directive. Article 4 defines an "identifiable natural person" as "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier ...". Recital 26 further provides that, in ascertaining whether means are reasonably likely to be used to identify the natural person, "account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments." It further explains that "[t]he principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

B. Directive 2002/58/EC

56. In addition, specifically for the field of electronic communications, 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 2002 L 201, p. 37) was adopted on 12 July 2002. It does not apply to the area of police and criminal justice but harmonises the provisions of the member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communications sector. Article 2 provides a definition of a "user" as meaning "any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service". It further defines "traffic data" as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". Moreover, it defines "communication" as "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service".

C. Council Framework Decision 2008/977/JHA and Directive (EU) 2016/680

57. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350, p. 60, hereinafter "Data Protection Framework Decision") aims at providing protection of personal data of natural persons when their personal data are processed for the purpose of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty. The Data Protection Framework Decision relies to a large extent on the principles and definitions which are contained in the 1981 Convention and in the Data Protection Directive.

58. 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 2016 L 119, p. 89) governs the handling of data by competent authorities, such as police and criminal justice authorities, for the purposes of, *inter alia*, investigation and prosecution of criminal offence. Article 3(1) contains the same definition of "identifiable natural person" and recital 21 the same explanation concerning the means of identification as the General Data

Protection Regulation (see paragraph 55 above). Furthermore, Article 4 requires that personal data should be, *inter alia*, processed lawfully and fairly. Article 1 (3) provides that member States may provide for higher safeguards than those contained in the directive.

59. The directive replaces Framework Decision 2008/977/JHA with effect from 6 May 2018.

D. Selected decisions of the Court of Justice of the European Union

60. As regards the concept of "personal data" under Article 2(a) of the Data Protection Directive, the Court of Justice of the European Union (CJEU) found in a judgment of 24 November 2011 in *Scarlet Extended*, C-70/10, EU:C:2011:771, paragraph 51, that users' IP addresses "were protected personal data because they allow those users to be precisely identified".

61. In its judgment of 19 October 2016 in *Breyer*, C-582/14, EU:C:2016:779, the CJEU dealt with the question of the specific character of dynamic IP addresses. It noted as follows:

> "[15] IP addresses are series of digits assigned to networked computers to facilitate their communication over the internet. When a website is accessed, the IP address of the computer seeking access is communicated to the server on which the website consulted is stored. That connection is necessary so that the data accessed maybe transferred to the correct recipient.
>
> [16] Furthermore, it is clear from the order for the reference and the documents before the Court that internet service providers allocate to the computers of internet users either a 'static' IP address or a 'dynamic' IP address, that is to say an IP address which changes each time there is a new connection to the internet. Unlike static IP addresses, dynamic IP addresses do not enable a link to be established, through files accessible to the public, between a given computer and the physical connection to the network used by the internet service provider."

62. The CJEU was of the view that a dynamic IP address did not constitute information relating to an "identified natural person", since such an address did not directly reveal the identity of the natural person who owned the computer from which a website had been accessed, or that of another person who might have used that computer (ibid, § 38). The CJEU went on to determine whether a dynamic IP address, in that case registered by an online media service provider, may be treated as data relating to an "identifiable natural person" within the meaning of Article 2(a) of the Data Protection Directive. For that purpose the CJEU, relying on recital 26, considered whether the possibility to combine the dynamic IP address, which was in the case at issue in the hands of the online media service provider, with the additional data held by the ISP constituted a means likely reasonably to be used to identify the data subject (§§ 41 and 45). The ECJU drew the following conclusion on that point:

"[49] Having regard to all the foregoing considerations, the answer to the first question is that Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."

V. COMPARATIVE LAW

A. German Federal Constitutional Court

63. The applicant referred to the judgment of the German Federal Constitutional Court ("the GFCC") of 24 January 2012, BVerfG, 1 BvR 1299/05. The GFCC partly upheld complaints concerning, *inter alia*, manual retrieval of information on dynamic IP addresses stored by the telecommunications service providers.

64. Under section 113 of the Telecommunications Act ("the TCA") the telecommunications service providers were required to supply, at the request of the competent (including law-enforcement) agencies, information on certain data collected, for the purpose of, *inter alia*, prosecuting criminal offences or regulatory offences. The impugned statutory provision was designed to be able to attribute if possible all telecommunications numbers to their respective subscribers (and in addition, ultimately, if possible, to their users). As found by the GFCC, the provision gave no specific thresholds of encroachment which would have defined its scope in more detail. Instead, it always permitted information in the individual case if this was necessary to perform the aforementioned duties. The GFCC did not find this in itself unconstitutional. However, the question that also arose was whether the impugned provision also covered information on the owner of a dynamic IP address. At the outset, the GFCC addressed the issue of a link between the subscriber information and the pre-existing content information which could be attributed to it. It found as follows (§113, a citation from a translation provided on the GFCC's website):

" ... the secrecy of telecommunications [Article 10.1 of the Basic Law] does not protect the confidentiality of the circumstances of each provision of telecommunications services, such as for example the attribution of the telecommunications numbers allocated by the service providers to particular subscribers."

65. The GFCC went on to note the distinction between static and dynamic IP addresses, finding as follows (§§ 115 and 116):

"... the attribution of a static IP address to a particular subscriber – more precisely, to a network interface of the subscriber – as a rule also gives indirect information on a particular telecommunications event involving the person in question, since such addresses, even if they are static, are registered and become the subject of attributions

identifying an individual almost only in connection with specific communications events. However, here too the conveying of information in this connection is as such limited exclusively to the abstract attribution of number and subscriber.

... In contrast, the situation is different when dynamic IP addresses are attributed to identified persons, for such addresses are particularly closely related to specific telecommunications events. This attribution is within the area of protection of Article 10.1 of the Basic Law. However, here too this does not automatically follow from the fact that the attribution of a dynamic IP address necessarily always relates to a specific telecommunications event of which it therefore indirectly also provides information. For in this connection too the information itself only relates to data which are abstractly attributed to a subscriber. There is therefore no fundamental difference from the attribution of static IP addresses. However, the application of Article 10.1 of the Basic Law is here based on the fact that when the telecommunications enterprises identify a dynamic IP address, they have to take an intermediate step, in which they examine the relevant connection data of their customers, that is, [they] must access specific telecommunications events. These telecommunications connections individually stored by the service providers are subject to the secrecy of telecommunications, irrespective of whether they have to be kept available by the service providers under a statutory duty ... or whether they are stored by them on a contractual basis. Insofar as the legislature imposes a duty on the telecommunications enterprises to access these data and to evaluate them in the interest of the state's performance of its duties, this is an encroachment upon Article 10.1 of the Basic Law. This is the case not only if the service providers must supply the connection data themselves, but also if they have to use the data as a preliminary question for information."

66. The GFCC concluded that section 113.1 of the TCA was in breach of Article 10.1 of the Basic Law to the extent that it was a basis for the supply of information on dynamic IP addresses.

67. Furthermore, although the GFCC did not find automated retrieval of data (section 12 of the TCA) concerning the static IP address unconstitutional, such a finding was made against the limited use of such addresses in the following context (§§ 160 and 161):

"... The allocation of static IP addresses, whose attribution is at present in any case publicly accessibly in practice, is essentially restricted to institutions and large-scale users. The possibility of retrieving such numbers has little weight in these circumstances.

However, § 112 TKG [TCA] may acquire substantially greater weight of encroachment if static IP addresses in future – for example on the basis of Internet Protocol Version 6 – should become more widely used as the basis of internet communication. For the question of the weight of encroachment of the identification of an IP address does not primarily depend – even if a number of fundamental rights apply in this case – on whether an IP address is technically dynamic or static, but on the actual significance of the creation of a duty of information in this connection. But if in practice static IP addresses are allocated to a great extent to private persons too, this may possibly mean that the identities of internet users are broadly or at least largely determined and that communications events in the internet are de-anonymised not only for a limited period of time, but permanently. Such a far-reaching possibility of de-anonymisation of communication in the internet goes beyond the effect of a traditional telephone number register. ... [T]he weight for the person affected of the

attribution of an IP address to a subscriber may not be equated to that of the identification of a telephone number, because the former makes it possible to access information whose scope and content are substantially more far-reaching .... In view of this increased information potential, the general possibility of the identification of IP addresses would only be constitutionally permissible subject to narrower limits ..."

B. The Canadian Supreme Court

68. The *R v. Spencer* (2014 SCC 43, [2014] 2 S.C.R. 212) case concerned the retrieval, without prior judicial authorisation, of the appellant's sister's subscriber information associated with a dynamic IP address, which the police had obtained in relation to online file-sharing involving child pornography. On the basis of the subscriber information received from the ISP, the police obtained a search warrant against the appellant. The latter sought to exclude the evidence found on his computer on the basis that the police actions in obtaining his address from the ISP without prior judicial authorisation amounted to an unreasonable search contrary to the Canadian Charter of Rights and Freedom. The judgment of the Supreme Court of Canada ("the SCC") of 13 June 2014, finding in favour of the appellant, was delivered by Judge Cromwell.

69. Referring to the previous case-law on the matter, the judgment noted that the reasonable expectation of privacy standard was normative rather than simply descriptive and that it was inevitably "laden with value judgments which [were] made from the independent perspective of the reasonable and informed person who [was] concerned about the long-term consequences of government action for the protection of privacy" (§ 18). The SCC, contrary to the opinion of the trial judge, found that the appellant's subjective expectation of privacy was justified by the fact that he had been the one using the network connection to transmit sensitive information. The judgment went on to determine whether the appellant's subjective expectation of privacy had been reasonable. For that purpose the judgment looked at two circumstances: the nature of the privacy interest at stake and the statutory and contractual framework governing the ISP's disclosure of subscriber information. As to the former, Judge Cromwell drew the following conclusions:

"[31 Thus, it is clear that the tendency of information sought to support inferences in relation to other personal information must be taken into account in characterizing the subject matter of the search.

[36] ... The analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought...

[41] There is also a third conception of informational privacy that is particularly important in the context of Internet usage. This is the understanding of privacy as anonymity. In my view, the concept of privacy potentially protected by s. 8 [right to

be secure against unreasonable search or seizure] must include this understanding of privacy.

[50] ... In the circumstances of this case, the police request to link a given IP address to subscriber information was in effect a request to link a specific person (or a limited number of persons in the case of shared Internet services) to specific online activities. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized by the Court in other circumstances as engaging significant privacy interests....

[51] I conclude therefore that the police request to Shaw [ISP] for subscriber information corresponding to specifically observed, anonymous Internet activity engages a high level of informational privacy. I agree with Caldwell J.A.'s conclusion on this point:

> . . . a reasonable and informed person concerned about the protection of privacy would expect one's activities on one's own computer used in one's own home would be private. . . . In my judgment, it matters not that the personal attributes of the Disclosed Information pertained to Mr. Spencer's sister because Mr. Spencer was personally and directly exposed to the consequences of the police conduct in this case. As such, the police conduct *prima facie* engaged a personal privacy right of Mr. Spencer and, in this respect, his interest in the privacy of the Disclosed Information was direct and personal..."

70. The judgment also answered the concerns of the prosecution authorities to the effect that recognising a right to online anonymity would carve out a crime-friendly Internet landscape. While acknowledging that this concern could not be taken lightly, Judge Cromwell explained that recognising an interest could not be equated to a right to anonymity and that in the present case, for example, it had seemed clear that the police could have easily obtained a production order for the subscriber information.

71. As regards the question whether the expectation of privacy was reasonable in the face of the relevant contractual and statutory provisions, the judgment found that the ISP's collection, use and disclosure of the personal information of its subscribers had been subject to the Personal Information Protection and Electronic Documents Act ("PIPEDA"), which protected personal information held by organisations engaged in commercial activity from being disclosed without the knowledge or consent of the person to whom the information related. The judgment found as follows:

> "[62] Section 7(3) (*c.*1)(ii) allows for disclosure without consent to a government institution where that institution has identified its *lawful authority* to obtain the information. But the issue is whether there was such lawful authority which in turn depends in part on whether there was a reasonable expectation of privacy with respect to the subscriber information. *PIPEDA* thus cannot be used as a factor to weigh against the existence of a reasonable expectation of privacy ... Given that the purpose of *PIPEDA* is to establish rules governing, among other things, disclosure "of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information" (s. 3), it would be reasonable for an

Internet user to expect that a simple request by police would not trigger an obligation to disclose personal information or defeat *PIPEDA* 's general prohibition on the disclosure of personal information without consent."

72. The judgment went on to establish that the police request had had no lawful authority and that the information had therefore been obtained unconstitutionally. The court refused to draw a parallel with other police routine inquires, such as an interview with the victim of a crime. Referring to *R. v. Duarte*, [1990] 1 S.C.R. 30, it found as follows:

"[67] ... In *Duarte*, the Court distinguished between a person repeating a conversation with a suspect to the police and the police procuring an audio recording of the same conversation. The Court held that the danger is 'not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words'... Similarly in this case, the police request that the ISP disclose the subscriber information was in effect a request to link Mr. Spencer with precise online activity that had been the subject of monitoring by the police and thus engaged a more significant privacy interest than a simple question posed by the police in the course of an investigation."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

73. The applicant complained that his right to privacy had been breached because (i) the Internet service provider (hereinafter "the ISP") had retained his alleged personal data unlawfully and (ii) the police had obtained subscriber data associated with his dynamic IP address and consequently his identity arbitrarily, without a court order, in breach of Article 8 of the Convention, which reads as follows:

"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."

A. Admissibility

1. As regards the alleged unlawful retention of personal data by the Internet service provider (ISP)

74. The Government argued that the applicant had failed to complain to the domestic courts of the unlawful retention of his personal data by the

ISP. Consequently, the domestic courts had not addressed this issue in the impugned decisions. They further argued that as the ISP was a private entity, the applicant could have sued it for damages in civil proceedings. One way or another, this part of the application should, in their view, be declared inadmissible for non-exhaustion.

75. In addition, the Government maintained that the applicant could not claim to be a victim of the alleged violation of Article 8 concerning the retention of the personal data, as those data had not concerned him but the Internet service subscriber, which was his father.

76. The applicant argued that the ISP had retained his personal data for almost six months without having a clear legal basis for such action and thus in violation of Article 8 of the Convention. In his observations, submitted on 15 October 2015, the applicant claimed that he had lodged his application with the Court not because the ISP had failed to keep his personal data secret or because it had retained them beyond the statutory time-limit, but because the State had obtained and used the data in question in the criminal proceedings against him. He argued that he had maintained, throughout the criminal proceedings, that the courts had relied on illegally obtained evidence.

77. The Court notes that the Government objected to the applicant's victim status with respect to this complaint. However, it does not consider it necessary to address this objection because this part of the application is in any event inadmissible for the following reasons.

78. The Court observes that the purpose of Article 35 § 1 is to afford the Contracting States the opportunity of preventing or putting right the violations alleged against them before those allegations are submitted to the Convention institutions. That rule is an important aspect of the principle that the machinery of protection established by the Convention is subsidiary to the national systems safeguarding human rights. Thus the complaint intended to be made subsequently to the Court must first have been made – at least in substance – to the appropriate domestic body, and in compliance with the formal requirements and time-limits laid down in domestic law (see, among other authorities, *Sejdovic v. Italy* [GC], no. 56581/00, §§ 43-44, ECHR 2006-II).

79. In the present case, the applicant complained in his application to the Court of the retention by the ISP of what he alleged were his personal data. However, he has failed to exhaust domestic remedies in this regard as he had not made this complaint – at least in substance – in the domestic proceedings.

80. Consequently, this part of the application should be declared inadmissible under Article 35 §§ 1 and 4 of the Convention.

2. As regards the disclosure of the subscriber information

81. The Government argued that the applicant could not claim to be a victim because the subscriber information that the ISP had disclosed to the police concerned his father.

82. The applicant disputed that view. He argued that it was his privacy that had been breached, not the subscriber's, and that the issue at stake was not that of ownership but that of the right to privacy.

83. The Court notes that this issue is closely related to the merits of the complaint and therefore joins the Government's objection to the merits.

84. It considers that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) The applicant

85. The applicant referred to the definition of personal data in the 1981 Convention (see paragraph 46 above), arguing that the obtaining of data without a court order (see paragraph 7 above) had led to his identification.

86. He also argued that although he had disclosed the contents of his communication to an unidentifiable public, he had not waived his right to privacy with regard to traffic (metering) data, that is data relating to the length and time of the use of the Internet and data relating to who used the Internet and what site he or she accessed during that use. In his view, such data enjoyed separate protection under the concept of private life, comprising the privacy of communications and informational privacy.

87. He submitted in this connection that the significant distinction between static and dynamic IP addresses should be recognised. While it might be possible to draw an analogy between a static IP address which was permanently attributed to the device, and a telephone number, a dynamic IP address was assigned every time the computer accessed the Internet. Referring to the German Federal Constitutional Court's judgment of 24 January 2012 (see paragraph 63 above), the applicant argued that by choosing a dynamic IP address, as had the subscriber in the present case, one chose to have his or her identity concealed, as additional data were required for identifying the computer used to access the Internet and thereby the subscriber. In his view, the dynamic IP address therefore fell within the scope of traffic data (metering), to which section 149b(1) applied.

88. The applicant further pointed out that the data on the content of communication had been obtained without the Slovenian authorities'

involvement. The Slovenian authorities would have needed a court order for obtaining such data, but had avoided that otherwise necessary step by requesting the subscriber information on the basis of section 149b(3) of the CPA. As regards the letter, the applicant alleged that at the time when the Slovenian police had obtained the data connecting his IP address to his identity, the law regulating access to such data had not been clear (*lex certa*) and therefore the lawfulness required by the second paragraph of Article 8 had not been met. In particular, at the time of the interference (August 2006), the domestic law provisions regarding this issue had been contradictory. The second paragraph of Article 37 of the Constitution required a court order for interference with the right to privacy of communication. The ECA provided that traffic data should be kept secret and that communication could be intercepted only on the basis of an order by a competent authority. In the domestic legal system that could only be a court order or, theoretically, a prosecution order. Anyhow, under section 107 it was possible only to "intercept" data and not to hand over certain retained data. Moreover, the providers were under an obligation to delete retained data pursuant to section 104 as soon as they no longer needed them for billing purposes. On the other hand, section 149b(1) and (3) of the CPA provided for different conditions of accessing data and it was unclear what the distinction in application between the two was. As a result of that uncertainty in the domestic legislation, one could not say that the legal protection against arbitrary interference by public authorities with the right to privacy was sufficient.

89. In the applicant's opinion, the ECA was *lex specialis* in relation to the CPA and it did not provide for a possibility to transfer personal data to the police. In such a situation of lacunae in the law, the Constitution should be applied directly, and the Constitution clearly required a court order for the transfer of such data.

(b) The Government

90. The Government explained that IP addresses were personal data and that likewise dynamic IP addresses were personal data but did not amount to traffic data. The only difference between the two was that the static IP address stayed with the subscriber as long as he did not change ISP, whereas a new dynamic IP address was assigned every time the subscriber accessed the Internet. With regard to both, the ISP stored data concerning the time of the use of a specific IP address.

91. The Government argued that the investigation had focused on the applicant only after the seizure and inspection of the computers had taken place and after those living at his address had been questioned. Thus the link between the subscriber and the applicant had become apparent only after the home search, which had been carried out on the basis of a valid court order.

92. While acknowledging that the IP address was an item of personal data because it allowed for the identification of an individual, the Government pointed out that it was each user's choice whether to use a website that allowed disclosure of personal data and/or content of communication to an unidentifiable and unlimited circle of individuals. The Government submitted that the applicant had not argued that he had hidden the IP address he had used to access the file-exchange program. As the disclosure of the IP address implied the disclosure of subscriber information, the applicant had not shown intent to keep his identity private or hidden and his right to private life was thus not engaged in the present case.

93. The Government argued that the applicant could not have expected that the subscriber information related to the dynamic IP address would have been withheld from the police. In their view, the contested measures had been lawful and proportionate to the aim of safeguarding the integrity of children, who, as particularly vulnerable individuals, enjoyed special protection under the Convention.

94. The Government drew a parallel with the situation where a suspect had been caught on closed-circuit television camera when driving. In such a situation, the suspect's photograph and his registration plates sufficed to identify him. Similarly, in the present case, it must be assumed that the moment the police had had the dynamic IP address and the timeline of its use, the user had been identified by way of such data. The Government thus argued that the domestic courts had correctly applied section 149b(3) instead of section 149b(1), as the latter concerned traffic data, not data concerning the owner or user of a communication device.

2. The Court's assessment

(a) Preliminary observations and scope of the Court's assessment

95. The Court at the outset observes the particular context of the present case, which concerns the disclosure of subscriber information associated with a dynamic IP address. It takes note of the extensive legislation and of the case-law concerning personal data protection and privacy of electronic communication within the European Union and will rely on them and on other relevant comparative-law material in assessing some of the technical matters applicable to the present case. It will also have regard, where appropriate, to the legal doctrines established therein.

96. As a preliminary matter, the Court further notes that an IP address is a unique number assigned to every device on a network, which allows the devices to communicate with each other. Unlike the static IP address, which is permanently allocated to a particular network interface of a particular device, a dynamic IP address is assigned to a device by the ISP temporarily, typically each time the device connects to the Internet (see paragraphs 61,

87 and 90 above). The IP address alone enables certain details, such as the ISP to which the user is connected and a broader physical location, most likely the location of the ISP, to be determined. Most dynamic IP addresses can thus be traced to the ISP and not to a specific computer. To obtain the name and address of the subscriber using a dynamic IP address, the ISP is normally required to look up this information and for that purpose to examine the relevant connection data of its subscribers (see paragraphs 61 and 65 above).

97. In the present case the information on the dynamic IP address and the time it had been assigned were collected by the Swiss police, who had carried out a monitoring exercise of users of the specific Internet network involving child pornography material. They forwarded the information to the Slovenian police, who obtained from the ISP the name and address of the subscriber associated with the dynamic IP address in question – the applicant's father (see paragraphs 6 and 7 above).

98. The Government argued that Article 8 of the Convention did not apply in this case because the applicant had not been directly affected by the contested measure and because even if he had been affected, he had willingly renounced his right to privacy by publicly exchanging the files in question (see paragraphs 92 and 93 above). In order to answer those questions, the Court must consider whether the applicant, or any other individual using the Internet, had a reasonable expectation that his otherwise public online activity would remain anonymous (see paragraphs 115 to 118 above).

99. The Court reiterates in this connection that sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims. Children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives, and that protection includes a need to identify the offenders and bring them to justice (see *K.U. v. Finland*, no. 2872/02, § 46, ECHR 2008-V). However, the questions raised by the Government concerning the applicability of Article 8 are to be answered independently from the legal or illegal character of the activity in question, as well as without any prejudice to the Convention's requirement that protection of vulnerable individuals must be provided by the member States, as pointed out in, amongst others, *K.U. v. Finland* (cited above).

(b) Applicability of Article 8

(i) Recapitulation of the relevant principles

100. The Court reiterates that private life is a broad term not susceptible to exhaustive definition. Article 8 protects, *inter alia*, the right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world. There is,

therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (see *Uzun v. Germany*, no. 35623/05, § 43, ECHR 2010-VI (extracts)).

101. There are a number of elements relevant to the consideration of whether a person's private life is concerned by measures affected outside his or her home or private premises. In order to ascertain whether the notions of "private life" and "correspondence" are applicable, the Court has on several occasions examined whether individuals had a reasonable expectation that their privacy would be respected and protected (see *Bărbulescu v. Romania* [GC], no. 61496/08, § 73, ECHR 2017, and *Copland v. the United Kingdom*, no. 62617/00, §§ 41- 42, ECHR 2007-I). In that context, it has stated that a reasonable expectation of privacy is a significant though not necessarily conclusive factor (see *Bărbulescu*, cited above, § 73).

102. In the context of personal data, the Court has pointed out that the term "private life" must not be interpreted restrictively. It has found that the broad interpretation corresponds with that of the 1981 Convention, the purpose of which is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1). Such personal data are defined as "any information relating to an identified or identifiable individual" (Article 2) (see *Amann v. Switzerland* [GC], no. 27798/95, § 65, ECHR 2000-II; see also paragraph 46 above).

103. It further follows from well-established case-law that where there has been a compilation of data on a particular individual, the processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private life considerations arise (see *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, § 136, ECHR 2017 (extracts)). Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged (ibid., § 137).

104. The Court has previously considered information such as metering data on the telephone numbers dialled (see *Malone v. the United Kingdom*, 2 August 1984, § 84, Series A no. 82), personal information relating to telephone, email and Internet usage (see *Copland*, cited above, §§ 41 and 43), information stored by the prosecution authorities on a card concerning the facts relating to the applicant's business relations (see *Amann*, cited above, § 66) and public information stored by the authorities on the applicant's distant past (see *Rotaru v. Romania* [GC], no. 28341/95, §§ 43 and 44, ECHR 2000-V) to fall within the ambit of Article 8.

105. Moreover, the Court has previously acknowledged in *Delfi AS v. Estonia* ([GC] no. 64569/09, § 147, ECHR 2015) the importance of online anonymity, noting that it has long been a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet. At the same time, the Court does not lose sight of the ease, scope and speed of the dissemination of information on the Internet, and the persistence of the information once disclosed, which may considerably aggravate the effects of unlawful speech on the Internet compared to traditional media (ibid.).

106. In the aforementioned case the Court elaborated also on different degrees of anonymity engaged in online activity and observed as follows (ibid., § 148):

> "The Court observes that different degrees of anonymity are possible on the Internet. An Internet user may be anonymous to the wider public while being identifiable by a service provider through an account or contact data that may be either unverified or subject to some kind of verification – ranging from limited verification (for example, through activation of an account via an e-mail address or a social network account) to secure authentication, be it by the use of national electronic identity cards or online banking authentication data allowing rather more secure identification of the user. A service provider may also allow an extensive degree of anonymity for its users, in which case the users are not required to identify themselves at all and they may only be traceable – to a limited extent – through the information retained by Internet access providers. The release of such information would usually require an injunction by the investigative or judicial authorities and would be subject to restrictive conditions. It may nevertheless be required in some cases in order to identify and prosecute perpetrators."

(ii) Application of the above principles to the present case

(α) Nature of the interest involved

107. The Government did not dispute that the subscriber information in principle concerned personal data (see paragraphs 90 and 92 above). Such a conclusion also follows from the definitions contained in the 1981 Convention, the legislation of the European Union, as well as domestic legislation aimed at their implementation (see paragraphs 40, 46, 53 and 57 above).

108. In addition, the Court notes that the subscriber information associated with specific dynamic IP addresses assigned at certain times was not publicly available and therefore could not be compared to the information found in the traditional telephone directory or public database of vehicle registration numbers referred to by the Government (see paragraph 94 above). Indeed, it would appear that in order to identify a subscriber to whom a particular dynamic IP address had been assigned at a particular time, the ISP must access stored data concerning particular telecommunication events (see, for instance, paragraphs 29, 61, 65 and 95

above). Use of such stored data may on its own give rise to private life considerations (see paragraph 103 above).

109. Furthermore, the Court cannot ignore the particular context in which the subscriber information was sought in the present case. The sole purpose of obtaining the subscriber information was to identify a particular person behind the independently collected content revealing data he had been sharing. The Court notes in this connection that there is a zone of interaction of a person with others which may fall within the scope of "private life" (see paragraph 100 above). Information on such activities engages the privacy aspect the moment it is linked to or attributed to an identified or identifiable individual (for reference to identifiability, albeit in a rather different context, see *Peck v. the United Kingdom*, no. 44647/98, § 62, ECHR 2003-I, and *J.S. v. the United Kingdom* (dec.), no. 445/10, §§ 70 and 72, 3 March 2015). Therefore what would appear to be peripheral information sought by the police, namely the name and address of a subscriber, must in situations such as the present one be treated as inextricably connected to the relevant pre-existing content revealing data (see the dissenting Constitutional Court judges' opinions cited in paragraphs 31 and 34; compare also with the position of the Canadian Supreme Court, cited in paragraphs 69 and 72 above, and the German Federal Constitutional Court, cited in paragraphs 64 and 65 above). To hold otherwise would be to deny the necessary protection to information which might reveal a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle.

110. In view of the above considerations, the Court concludes that the present case concerns privacy issues capable of engaging the protection of Article 8 of the Convention.

(β) Whether the applicant was identified by the contested measure

111. The Court must next address the Government's argument that the subscriber information obtained by the police disclosed only the name and address of the applicant's father, and not the applicant (see paragraph 91 above). In this connection, the Court observes that it has been generally accepted that the definition of personal data refers to information relating not only to identified but also to identifiable individuals (see paragraphs 40, 47, 53, 54, 55 and 58 above).

112. In the present context, the applicant was no doubt the user of the Internet service in question (see paragraph 56 above) and it was his online activity that was monitored by the police. The Court further observes that the applicant used the Internet by means of what would appear to be his own computer at his own home. It is of little significance that the applicant's name was not mentioned in the subscriber information obtained by the police. Indeed, it is not unusual for one household to have a single

subscription to the Internet service used by several members of the family. The fact that they are not personally subscribed to the Internet service has no effect on their privacy expectations, which are indirectly engaged once the subscriber information relating to their private use of the Internet is revealed.

113. It is clear that the purpose of the contested measure, that is the obtaining by the police, without a court order, of subscriber information associated with the dynamic IP address provided by the Swiss police (see paragraph 7 above), was to connect the computer usage to a location and, potentially, to a person. The subscriber information, which contained also the address, allowed the police to identify the home from which the Internet connections in question had been made. This led them to identify the applicant as the then suspected user of the Razorback network.

114. Having regard to the foregoing and bearing also in mind that the domestic courts did not dismiss the case on the grounds that the applicant had not been the subscriber to the Internet service in question, the Court concludes that this fact cannot be taken as a bar to the application of Article 8 in the present case. It accordingly dismisses the Government's objection concerning the alleged lack of victim status (see paragraph 83 above).

(γ) Whether the applicant had a reasonable expectation of privacy

115. In order to ascertain whether the notion of a "private life" is applicable to the present case, it remains for the Court to examine whether, in view of the publicly accessible nature of the network in question, the applicant had a reasonable expectation that his privacy would be respected and protected (see paragraph 101 above). In this connection, the Slovenian Constitutional Court and the respondent Government (see paragraphs 14 and 18 of the Constitutional Court's decision, cited in paragraph 29 above; see also paragraph 92 above) found it important that the applicant had participated in the Razorback network to which access had not been restricted. They considered that he had knowingly exposed his online activity and associated dynamic IP address to the public. Thus, in their opinion, his expectation of privacy had not been legitimate and, moreover, he should have been considered to have waived it (ibid.).

116. The Court, like the Constitutional Court, accepts that the applicant, when exchanging files with pornographic material through the Razorback network, expected, from his subjective angle, that that activity would remain private and that his identity would not be disclosed (see paragraph 14 of the Constitutional Court's decision cited in paragraph 29 above). However, unlike the Constitutional Court, the Court considers that the fact that he did not hide his dynamic IP address, assuming that it is possible to do so, cannot be decisive in the assessment of whether his expectation of privacy was reasonable from an objective standpoint. In this connection, it

notes that the question is clearly not whether the applicant could have reasonably expected to keep his dynamic IP address private but whether he could have reasonably expected privacy in relation to his identity.

117. The Court has previously acknowledged the anonymity aspect of online privacy (see *Delfi AS*, cited in paragraph 105 above, see also paragraph 12 of the Constitutional Court's decision, cited in paragraph 29 above), relating to the nature of the online activity, in which the users participate without necessarily being identifiable. This anonymity conception of privacy is an important factor to be taken into account in the present assessment. In particular, it has not been argued that the applicant had ever disclosed his identity in relation to the online activity in question (see in this connection the dissenting opinion of Judge Jadek Pensa, cited in paragraph 33 above) or that he was for example identifiable by the particular website provider through an account or contact data. His online activity therefore engaged a high degree of anonymity (see *Delfi AS*, cited in paragraph 105 above, § 148), as confirmed by the fact that the assigned dynamic IP address, even if visible to other users of the network, could not be traced to the specific computer without the ISP's verification of data following a request from the police.

118. Lastly, the Court notes that the applicable legal and regulatory framework might also be a relevant, though not necessarily decisive, factor in determining the reasonable expectation of privacy (see, for instance, *J.S. v. the United Kingdom* (dec.), cited above, § 70, and *Peev v. Bulgaria*, no. 64209/01, § 39, 26 July 2007). In the present case, neither of the parties submitted information regarding the terms of the contract on the basis of which the Internet service had been provided to the applicant's father. As to the statutory framework, the Court finds it sufficient to note that Article 37 of the Constitution guaranteed the privacy of correspondence and of communications and required that any interference with this right be based on a court order (see paragraph 35 above). Therefore, also from the standpoint of the legislation in force at the relevant time, the applicant's expectation of privacy with respect to his online activity could not be said to be unwarranted or unreasonable.

(δ) Conclusion

119. For all of the above reasons, the Court concludes that the applicant's interest in having his identity with respect to his online activity protected falls with the scope of the notion of "private life" and that Article 8 is therefore applicable to this complaint.

(c) Compliance with Article 8

(i) Whether there was interference

120. Having regard to the above conclusion that the applicant's right to respect for his private life as guaranteed by Article 8 § 1 was engaged in the present case, the Court further finds it established that the police request to the ISP and their use of the subscriber information leading to the applicant's identification amounted to an interference with this right (see, *mutatis mutandis*, *Rotaru*, cited above, § 46, and *Uzun*, cited above, § 52). In view of the foregoing, it does not consider it necessary to determine whether the measure in question amounted also to an interference with the applicant's right to respect for his correspondence.

121. The Court must therefore examine whether the interference with the applicant's right to privacy was in conformity with the requirements of the second paragraph of Article 8, in other words whether it was "in accordance with the law", pursued one or more of the legitimate aims set out in that paragraph and was "necessary in a democratic society" to achieve the aim or aims in question.

(ii) Whether the interference was in accordance with the law

122. The Court notes that the expression "in accordance with the law", within the meaning of Article 8 § 2 requires firstly that the contested measure should have some basis in domestic law. Second, the domestic law must be accessible to the person concerned. Third, the person affected must be able to foresee the consequences of the domestic law for him, and fourth, the domestic law must be compatible with the rule of law (see, among many other authorities, *Rotaru*, cited above, § 52; *Liberty and Others v. the United Kingdom*, no. 58243/00, § 59, 1 July 2008; and *Sallinen and Others v. Finland*, no. 50882/99, § 76, 27 September 2005).

123. The Court also reiterates that it is primarily for the national authorities, notably the courts, to interpret and apply domestic law. However, the Court is required to verify whether the way in which the domestic law is interpreted and applied produces consequences that are consistent with the principles of the Convention as interpreted in the light of the Court's case-law (see *Cocchiarella v. Italy* [GC], no. 64886/01, §§ 81 and 82, ECHR 2006-V).

124. In the present case, assuming that the obtaining by the police of the subscriber information associated with the dynamic IP address in question had some basis in domestic law because section 149b(3) of the CPA provided that the police could obtain information on the owner or user of a certain means of electronic communication from the ISP (see paragraph 36 above), the Court must examine whether that law was accessible and foreseeable and compatible with the rule of law.

125. It notes that the present case raises no issues with respect to the accessibility of the law. As regards the remaining requirements, the Court reiterates that a rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct (see *Rotaru*, cited above, § 55 and the principles summarised therein). In addition, compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 rights (see, *mutatis mutandis*, *Amann*, cited above, §§ 76-77; *Bykov v. Russia* [GC], no. 4378/02, § 76, 10 March 2009; see also *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 94, ECHR 2006-XI; and *Liberty and Others*, cited above, § 62). The Court must thus be satisfied also that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (see *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 77, 28 June 2007, with reference to *Klass and Others v. Germany*, 6 September 1978, § 50, Series A no. 28, and *Uzun*, cited above, § 63).

126. Having regard to the particular context of the case, the Court would emphasise that the Cybercrime Convention obliges the States to make measures such as the real-time collection of traffic data and the issuing of production orders available to the authorities in combating, *inter alia*, crimes related to child pornography (see paragraphs 47 to 51 above). However, such measures are, pursuant to Article 15 of that Convention, "subject to conditions and safeguards provided for under [State parties'] domestic law" and must "as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure" (see paragraph 52 above).

127. In the present case, the Court notes that section 149b(3) of the CPA (see paragraph 36 above), relied on by the domestic authorities, concerned a request for information on the owner or user of a certain means of electronic communication. It did not contain specific rules as to the association between the dynamic IP address and subscriber information. The Court further notes that Article 37 of the Constitution required a court order for any interference with privacy of communication (see paragraph 35 above). Furthermore, the ECA (see paragraph 37 above), which specifically regulated the secrecy and confidentiality of electronic communication, did not at the relevant time provide for the possibility that subscriber information and related traffic data be accessed and transferred for the purposes of criminal proceedings. It provided that electronic

communications, including the related traffic data, were confidential and as such should be protected by the ISP (see paragraph 37 above). It further stipulated that the ISP should not transfer the traffic data to others unless this was necessary for the provision of the service, except where the lawful interception of communications had been ordered by the competent authority (see section 103 of the ECA, cited in paragraph 37 above). Therefore, the legislation was, at the very least, not coherent as regards the level of protection afforded to the applicant's privacy interest.

128. Having said that, the Court would be usurping the function of national courts were it to attempt to make an authoritative statement as to which law should have prevailed in the present case. It must instead turn to the reasoning offered by the domestic courts. It notes in this connection that the Constitutional Court considered that the "identity of the communicating individual [was] one of the important aspects of communication privacy" and that its disclosure required a court order pursuant to paragraph 2 of Article 37 of the Constitution (see paragraph 18 of the Constitutional Court's decision, cited in paragraph 29 above). More specifically, according to the Constitutional Court's interpretation, which was consistent with its previous case-law finding that the traffic data, as defined under the domestic law, fell within the protection of Article 37 of the Constitution (ibid.), the disclosure of subscriber information associated with a certain dynamic IP address in principle required a court order and could not be obtained by means of a simple written request by the police.

129. The Court observes that, indeed, the only reason for the Constitutional Court dismissing the applicant's complaint – that is, for approving of the disclosure of the subscriber information without a court order – was the presumption that the applicant had "waived the legitimate expectation of privacy" (see paragraph 18 of the Constitutional Court's decision, cited in paragraph 29 above). However, the Court, having regard to its findings in the context of the applicability of Article 8, does not find the Constitutional Court's position on that question to be reconcilable with the scope of the right to privacy under the Convention (see paragraphs 115 to 118 above). Bearing in mind the Constitutional Court's finding that the "identity of the communicating individual" fell within the scope of the protection of Article 37 of the Constitution (see paragraph 128 above) and the Court's conclusion that the applicant had a reasonable expectation that his identity with respect to his online activity would remain private (see paragraphs 115 to 118 above), a court order was necessary in the present case. Moreover, nothing in the domestic law prevented the police from obtaining it given that they, a few months after obtaining the subscriber information, during which time apparently no investigative steps had been taken in the case, requested and obtained a court order for what would seem to be, at least in part, the same information as that which had already been in their possession (see paragraph 8 above). The domestic authorities'

reliance on section 149b(3) of the CPA was therefore manifestly inappropriate and, what is more, it offered virtually no protection from arbitrary interference.

130. In this connection, the Court notes that at the relevant time there appears to have been no regulation specifying the conditions for the retention of data obtained under section 149b(3) of the CPA and no safeguards against abuse by State officials in the procedure for access to and transfer of such data. As regards the latter, the police, having at their disposal information on a particular online activity, could have identified an author by merely asking the ISP provider to look up that information. Furthermore no independent supervision of the use of these police powers has been shown to have existed at the relevant time, despite the fact that those powers, as interpreted by the domestic courts, compelled the ISP to retrieve the stored connection data and enabled the police to associate a great deal of information concerning online activity with a particular individual without his or her consent (see paragraphs 108 and 109 above).

131. The Court further notes that soon after the contested measure had been taken against the applicant, the Parliament adopted amendments to the ECA (see paragraph 38 above, as well as the relevant provisions in the subsequent new law cited in paragraph 39). Those amendments provided, among other things, rules on the retention of data concerning the origin of communications, that is, *inter alia*, the name and address of the subscriber to whom a certain IP address had been assigned, and the procedure for accessing and transferring them. This, however, had no effect on the applicant's situation.

132. Bearing in mind the above, the Court is of the view that the law on which the contested measure, that is the obtaining by the police of subscriber information associated with the dynamic IP address in question (see paragraph 7 above), was based and the way it was applied by the domestic courts lacked clarity and did not offer sufficient safeguards against arbitrary interference with Article 8 rights.

133. In these circumstances, the Court finds that the interference with the applicant's right to respect for his private life was not "in accordance with the law" as required by Article 8 § 2 of the Convention. Consequently, the Court need not examine whether the contested measure had a legitimate aim and was proportionate.

134. Having considered all of the above, the Court concludes that there has been a violation of Article 8 of the Convention.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

135. Article 41 of the Convention provides:

"If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

136. The applicant claimed 32,000 euros (EUR) in respect of non-pecuniary damage, which included EUR 7,000 for the distress he had suffered because of the trial against him, EUR 15,000 because he had been unjustifiably imprisoned and EUR 10,000 for the stigmatisation he had suffered in the society as a result of his conviction.

137. The Government argued that the applicant's claim for non-pecuniary damage was unsubstantiated and excessive. They further argued that there was no connection between the violation of Article 8 alleged in the present case and the alleged non-pecuniary damage in relation to the applicant's criminal conviction and prison sentence. In particular, even if the information in question had been excluded from the file, the applicant could not have avoided the criminal proceedings against him. Moreover, the Government maintained that as the applicant had admitted that he could request the reopening of the proceedings in the event of the finding of a violation, a declaratory finding by the Court should suffice.

138. The Court considers that the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage that may have been sustained by the applicant.

B. Costs and expenses

139. The applicant also claimed EUR 4,335.50 for the costs and expenses incurred before the domestic courts and EUR 2,600 for those incurred before the Court plus value-added tax (VAT). He argued that those sums had been calculated on the basis of the official tariff for lawyers.

140. The Government argued that the costs the applicant had claimed with respect to his representation in the domestic proceedings included VAT. They also included the costs of a legal opinion, namely EUR 2,000, which had clearly not been produced for the purposes of the domestic proceedings. As regards the claim for the cost of the proceedings before the Court, the Government argued that it was excessive. Moreover, except for the bill for the aforementioned legal opinion, the applicant had not submitted any evidence that he had incurred costs on account of his legal representation.

141. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as

to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 922 for costs and expenses in the domestic proceedings and EUR 2,600 for the proceedings before the Court. In total, he should thus be awarded EUR 3,522 for costs and expenses.

C. Default interest

142. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT

1. *Decides*, by six votes to one, to join to the merits the Government's objection of the lack of victim status concerning the disclosure of the subscriber information under Article 8 of the Convention and *rejects* it;

2. *Declares*, by a majority, the complaint concerning the disclosure of the subscriber information under Article 8 of the Convention admissible and the remainder of the application inadmissible;

3. *Holds*, by six votes to one, that there has been a violation of Article 8 of the Convention;

4. *Holds*, unanimously, that the finding of a violation constitutes in itself sufficient just satisfaction for the non-pecuniary damage sustained by the applicant;

5. *Holds*, by six votes to one,
   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, EUR 3,522 (three thousand five hundred and twenty-two euros) plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

Done in English, and notified in writing on 24 April 2018, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Andrea Tamietti
Deputy Registrar

Ganna Yudkivska
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) Concurring opinion of Judge G. Yudkivska, joined by Judge M. Bošnjak;

(b) Dissenting opinion of Judge F. Vehabović.

G.Y.
A.N.T.

CONCURRING OPINION OF JUDGE YUDKIVSKA, JOINED BY JUDGE BOŠNJAK

I agree with the outcome of the judgment as well as with the methodology used by the majority. What surprises me, however, is the apparent difficulty with which the conclusion on the existence of interference in this case is reached and, in particular, a very cautious approach to the reasonable expectation of privacy in paragraphs 115-118.

The case in issue presented a unique opportunity to clarify the scope of the reasonable expectation of privacy in the digital age, where a striking amount of information about our private lives is easily circulated beyond our control. "Civilization is the progress toward a society of privacy", stated Ayn Rand[1]. The modern reality, however, is that privacy is increasingly becoming a cherished value, which requires greater protection day by day. Countless scholars have already announced the "death", "end" or "destruction" of privacy[2]. It is argued that in order to protect privacy in the modern era we must reconsider the outdated understanding of it as mere secrecy, and move toward legal protection of trust and confidentiality and of the right to control how information is disseminated and used[3]. As judges we are entrusted with the task of rethinking the privacy paradigm in cases such as the present one.

For the first time in this case the Court has gone into a study of the Internet Protocol and forms of IP addressing, namely static and dynamic – to the extent necessary in the circumstances. In *Benedik* we are dealing with dynamic IP addressing, that is, assigning new IP addresses at random from a pool of addresses assigned to an Internet service provider on each occasion that a user connects to the internet. Today dynamic IP addressing is the most common form for Internet consumers, and therefore the Court's conclusions on privacy in the present case will affect the great majority of internet users all around Europe.

It has become commonplace to recall in privacy discussions that the legal notion of privacy was not pronounced until Samuel D. Warren and Louis D. Brandeis published their prominent article "The Right to Privacy" back in 1890. What deserves to be mentioned is that they were prompted by concern that modern technologies, namely the recently invented portable camera and the rapid development of printed media, would reveal unwanted details about the lives of ordinary people: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the

1. Ayn Rand, The Fountainhead.
2. See Daniel Solove, "Speech, Privacy and Reputation on the Internet" at: Saul Levmore and Martha Nussbaum, Eds., The Offensive Internet: Speech, Privacy, and Reputation, Cambridge, Mass.: Harvard University Press, 2011, with further references.
3. Ibid., pp. 20 and 22.

prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'."[4]

Since that time, every development in existing technologies and the appearance of new ones has generated a revisiting of the doctrine of privacy and its reasonable expectations: from concerns about monitoring of telephone conversations at the beginning of the 20th century to wide discussions on mass surveillance, collection and processing of metadata at the beginning of the 21st century. Yet in 1966 Justice William Douglas in his dissenting opinion in *Osborn v. United States* warned: "We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government"[5]. The technical possibilities that exist nowadays are far more intrusive than Justice Douglas could even have imagined some fifty years ago. But the wide expansion of the internet merely presents a new degree of intensity in respect of an old problem.

The notion of a "reasonable expectation of privacy" has been used by the Court in several cases, including the present one, but this notion came to us from the United States Supreme Court, where it appeared in the case of *Katz v. United States*[6], which concerned the use by the FBI of eavesdropping devices for receiving conversations on illegal gambling made by a suspect from a public telephone booth. As the Supreme Court observed, "no less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."

It was a concurring opinion by Justice Harlan which introduced this particular concept: he wrote that his "understanding of the rule that has emerged from prior decisions is that there is a twofold requirement": (1) a person "has demonstrated the actual (subjective) expectation of privacy", and (2) society is ready to admit that this expectation is (objectively) reasonable. It is this test which has subsequently been cited in the Supreme Court's Fourth Amendment case-law.

The concept of a "reasonable expectation of privacy" was first used by this Court in *Halford v. the United Kingdom*[7]. There, the Court concluded that a police officer had reasonable expectations about the privacy of phone calls made at the workplace, in the absence of any warning that those calls could be intercepted. The Court referred to the same concept ten years later

4. Warren & Brandeis, the Right to Privacy, 4 HARV. L. REV. 193 (1890).
5. Osborn v. United States, 385 U.S. 323 (1966).
6. Katz v. United States, 389 U.S. 347 (1967).
7. *Halford v. the United Kingdom*, 25 June 1997, *Reports of Judgments and Decisions* 1997-III.

in *Copland v. the United Kingdom*[8], finding that, in the absence of any warning, a college employee also had reasonable expectations about the privacy of the emails she had sent from her college mailbox account.

More recently, the concept was mentioned in the Grand Chamber case of *Bărbulescu v. Romania*[9]. The case concerned the applicant's dismissal following the monitoring of his electronic communications, mainly through his Yahoo Messenger account, which the applicant was instructed to create for communicating with clients. It was found that he used the Internet for personal purposes during the working day, in violation of internal rules. The Court left open the question of whether the applicant had a reasonable expectation of privacy, notwithstanding the employer's clear instructions for abstaining from any personal activity in the workplace, because an "employer's instructions cannot reduce private social life in the workplace to zero".

The present case raises the issue of a reasonable expectation of privacy when it comes to traffic data (metering or metadata), and I regret that the Court missed the opportunity to take a clear stance on it. An interesting discussion of this topic within the Constitutional Court of Slovenia (see paragraphs 28-34 of the judgment) was left unaddressed.

Similar discussions are ongoing among the American judiciary. Under the original conception of US constitutional law, the Supreme Court has clearly proceeded on the basis that while there can be said to be a reasonable expectation of privacy with respect to content, there is no such expectation when it comes to metadata (traffic data). Some forty years ago, in the case of *Smith v. Maryland*[10], the Supreme Court considered the handling of metadata by telephone companies, which have information on the numbers dialled and the duration of conversations. It observed that "it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret." Under this concept, therefore, an individual does not have a reasonable expectation of privacy with regard to this type of information.

American courts have interpreted the "third-party doctrine" established in *Smith* to apply to IP addresses, and have held that Internet users have no reasonable expectation of privacy in their IP addresses because they are voluntarily conveyed to third parties - the users' ISPs and web service providers[11], noting, however, that "the mere act of accessing a network does

8. *Copland v. the United Kingdom*, no. 62617/00, ECHR 2007-I.
9. GC, no. 61496/08, ECHR 2017 (extracts).
10. Smith v. Maryland, 442 U.S. 735 (1979).
11. See Alexandra D. Vesalga, Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data, 43 GOLDEN GATE U.L.REV. 459(2013), referring to United States v. Bynum, 604 F.3d 161, 164 & n.2 (4th Cir. 2010); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); United States v. Forrester, 512 F.3d 500, 509-10 (9th Cir. 2008), etc.

not in itself extinguish privacy expectations"[12] and that "individuals possess objectively reasonable expectations of privacy in the contents of their computers"[13]. Nevertheless, in 2008 the Superior Court of New Jersey adopted the judgment in the case of *State v. Reid*[14], explaining that "individuals need an ISP address in order to access the Internet. However, when users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential. Many are unaware that a numerical IP address can be captured by the websites they visit. More sophisticated users understand that that unique string of numbers, standing alone, reveals little if anything to the outside world. Only an Internet service provider can translate an IP address into a user's name."

The NJ Court then proceeded with a crucially important reshaping of the privacy pattern, prompted by modern internet activities: "... while decoded IP addresses do not reveal the content of Internet communications, subscriber information alone can tell a great deal about a person. With a complete listing of IP addresses, one can track a person's Internet usage... Such information can reveal intimate details about one's personal affairs in the same way as disclosure of telephone billing records does. Although the contents of Internet communications may be even more revealing, both types of information implicate privacy interests".

In my view, this is the key challenge to be clearly articulated – traffic data or metadata is collected nowadays much more broadly than the content data (actual content of communications), and such interference must be "established beforehand in a law, and set forth expressly, exhaustively, precisely, and clearly, both substantively and procedurally", defining "the causes and conditions that would enable the State to intercept the communications of individuals, collect communications data or "metadata," or to subject them to surveillance or monitoring that invades spheres in which they have reasonable expectations of privacy."[15]. The PACE Resolution on Mass Surveillance[16] urged the Council of Europe member States "to ensure that their national laws only allow for the collection and analysis of personal data (*including so-called metadata*) with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity...".

It appears accepted that the collection of metadata was seen (and is still seen) as less intrusive than the collection of content. In the pre-internet era, in 1984, the European Court of Human Rights held that while collecting

12. United States v. Heckenkamp, 482 F.3d 1 142, 1 146 (9th Cir. 2007).
13. United States v. Howe, 2011 WL 2160472 at. 7 (W.D.N .Y. May 27, 2011).
14. State v. Reid, 945 A.2d 26, 28 (N.J. 2008).
15. The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013).
16. PACE Resolution on Mass Surveillance 2045 (21 April 2015).

content is a greater intrusion than collecting metadata, collecting metadata would still be an interference with Article 8. This was the case in *Malone v. the United Kingdom*[17], where the police used devices that recorded the numbers dialled on a particular phone, as well as the time and duration of each call - without interception of the conversations. The Government argued that the collection of such information did not entail an interference with the right guaranteed by Article 8.

The Court noted in *Malone* that it "does not accept ... that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8", as the numbers dialled were an "integral element in the communications made by telephone" and the handing over of that information from a telephone service provider to the police without the consent of the subscriber amounted to an interference with a right guaranteed by Article 8 (*Malone*, § 84).

This position needs to be substantially strengthened today. The view that metadata does not deserve the same level of protection as content data is shattered as it is confronted with present-day realities: there are currently so many forms of metadata - from phone calls, e-mails, web engines showing your surfing history, to Google Maps showing your location, etc.; and if this data are aggregated, an outstandingly intrusive portrait is obtained of the person concerned, revealing his or her personal and professional relationships, ethnic origin, political affiliation, religious beliefs, membership of different groups, financial status, shopping or disease history, and so on. In order to obtain this information, one need not go to the trouble of listening to conversations or reading letters, as in the good old days. This point was underlined in the United Nations Human Rights Council Resolution on the Right to Privacy in the Digital Age, which noted that "while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity"[18].

In his book "Data and Goliath"[19], specifically devoted to "the golden age of surveillance", leading security expert Bruce Schneier gives a fascinating example of an experiment conducted by Stanford University, which examined the phone metadata of a number of people and easily identified among them - using only traffic information about their various phone calls - a heart-attack victim, a home marijuana grower, and a pregnant woman planning an abortion.

---

17. *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82.
18. UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017).
19. Bruce Schneier, "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World", New York, N.Y.: W.W. Norton & Company, 2015.

The collection and aggregation of several types of protected information from various sources creates new risks for human rights, to which this Court cannot turn a blind eye, given that almost everything we do leaves a digital footprint.

The applicant in the present case, like all other internet users, enjoyed anonymity, as dynamic IP addresses can be linked to one's identity only if specifically disclosed by the service provider following a relevant request. Thus, there should be no doubt that his expectations of privacy were perfectly legitimate, notwithstanding the abhorrently illegal character of his activity as explained in paragraph 99 (had the interference been in accordance with the law the Court would have proceeded with a further examination of its proportionality and the nature of the crime would have been given due consideration).

In view of the foregoing, I believe that the Court ought to have stated unequivocally that, given the technical anonymity of IP addresses, internet users have reasonable expectations of privacy when surfing the Web. Further processing of this metadata may only be carried out in accordance with a law that satisfies quality requirements, as argued above.

Privacy protection is a crucial achievement in European political and legal culture, not least because it was formed against the backdrop of the horrors of the Nazi and communist regimes. In the long run, privacy will stand as a fundamental right only so long as it is defended by society, and it will disappear if society stops seeing it as essential value. We do have a reasonable expectation that our privacy will be protected even when we go online. Our fundamental right to control how we present ourselves to the outside world is vital, and this stance should be reinforced by the Court.

DISSENTING OPINION OF JUDGE VEHABOVIĆ

I did not vote with the majority, which found that there had been a violation of Article 8 of the Convention concerning the applicant's reasonable expectation of privacy and the existence of an interference with the applicant's rights under Article 8 of the Convention.

The information disclosed on 7 August 2006 to the local authorities by the Internet Service Provider (ISP) was not traffic data or personal information concerning the applicant; it was the address and the name of the applicant's father who was the subscriber to the internet service. It appears from that fact that the applicant could not claim to be a victim because the subscriber information which the ISP had disclosed to the police concerned his father, who is not the applicant in this case, as pointed out by the Government.

A reasonable suspicion of the transfer of files including child pornography, which is a criminal act, required the local authorities to investigate further, and the information concerning the applicant, that is to say traffic data relating to the internet activities made from this IP address, was revealed to the police on 14 December 2006 after the District Court had issued an order demanding that the ISP disclose both the personal data of the subscriber and traffic data linked to the IP address in question. In addition to that the investigating judge of the Kranj District Court on 12 January 2007 issued an order to carry out a house search and only then was the applicant connected to the traffic data in question and only from that moment can the applicant claim to be a victim.

In my opinion, the retrieved IP address which led to the address and the name of the applicant's father is not of sufficient proximity to qualify as the personal data of the applicant himself, as it revealed the identity and traffic data of neither the applicant nor his father.

The Court has on a number of occasions referred to the Data Protection Convention which defines personal data in Article 2 as "any information relating to an identified or identifiable individual", (see *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, 931/13, § 133, and *Amann v. Switzerland*, 27798/95, §65). Local authorities did not receive information on the applicant; the applicant was not an identified or an identifiable individual prior to the court order which was the basis for the Court's finding of a violation of Article 8 of the Convention. I therefore do not agree with the majority's finding that there was an interference contrary to the applicant's right under Article 8 of the Convention.

Concerning the reasonable expectation of privacy, I do not agree that the subjective angle of the applicant on his expectation for privacy should be taken into account where a criminal activity is under consideration. In nearly all cases, criminals would not wish their activities to be known to others. This kind of expectation of privacy would not be reasonable when

based on an unlawful, or in this case a criminal, incentive. An expectation to hide criminal activity should not be considered as reasonable. On a second issue concerning the reasonable expectation of privacy, the applicant exchanged files including child pornography (which the Chamber, in my opinion, intentionally omitted from § 115) through a public network account which was visible to others. The applicant therefore knew, or ought to have known, that his actions were not anonymous. The applicant did not intend to conceal his activity at the time of commission of the offence.

Furthermore, in many cases in which an interference was found, the Court considered the prevention of crime as constituting a legitimate aim. For example in *Nada v. Switzerland*, the Court decided that "[t]he applicant did not appear to deny that the impugned restrictions were imposed in pursuit of legitimate aims. The Court finds it established that those restrictions pursued one or more of the legitimate aims enumerated in Article 8 § 2: firstly, they sought to prevent crime" (*Nada v. Switzerland*, 10593/08, § 174). Also, in *S. and Marper v. the United Kingdom*, "[t]he Court agrees with the Government that the retention of fingerprint and DNA information pursues the legitimate purpose of the detection and, therefore, prevention of crime. While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the identification of future offenders" (see *S. and Marper v. the United Kingdom*, 30562/04 30566/04, § 100). For these reasons, I do not agree with the finding of the majority that there was a violation of the applicant's rights the under Article 8 of the Convention.