EHRC 2018/154

Dynamisch IP adres, Kinderporno, Reasonable expectation of privacy, Quality of the law

GEGEVENS

Instantie	Europees Hof voor de Rechten van de Mens
Datum uitspraak	24-04-2018
Publicatie	EHRC 2018/154 (Sdu European Human Rights Cases), aflevering 8, 2018
Annotator	dr. B. van der Sloot
Zaaknummer	62357/14
Rechtsgebied	Grondrechten
Rubriek	Uitspraken EHRM
Rechters	Yudkivska (President) De Gaetano Vehabovic Ranzoni Ravarani Bosnjak Paczolay
Partijen	Benedik tegen Slovenië
Regelgeving	-

SAMENVATTING

Een man van zo'n 40 jaar oud downloadt porno, waaronder kinderporno, via de internetverbinding van zijn vader. De internetverbinding werkt niet via een statisch IP-adres, waarbij een aansluiting één vast IP-adres heeft, maar via een dynamisch IP-adres, waarbij er steeds wanneer de computer opnieuw wordt opgestart een nieuw IP-adres wordt toegekend. De internetprovider houdt een logboek bij van welk dynamisch IP-adres bij welke gebruiker hoort. De politie wendt zich in casu tot de internetprovider om de identiteit en het adres van de internetgebruiker te achterhalen, omdat er via het dynamische IP-adres illegale activiteiten zijn ontplooid. Er zijn twee rechtsvragen. Ten eerste: is er een inbreuk gemaakt op de privacy van de man, nu door het opvragen van de gegevens over de gebruiker van het IP-adres de identiteit van de vader van de man en niet van de man

zelf is achterhaald? Ja, zegt het EHRM, er is in casu een inperking van art. 8 EVRM, waarin het recht op privacy is gewaarborgd. Ten tweede: was deze beperking voorgeschreven bij wet? Nee, zegt het EHRM, en dus is er niet voldaan aan de voorwaarden van art. 8 lid 2 EVRM en is er een schending van het recht op privacy.

UITSPRAAK

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 *Barbulescu 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 *Barbulescu*, 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.

(b) 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;

6. *Dismisses*, unanimously, the remainder of the applicant's claim for just satisfaction.

Concurring opinion of Judge Yudkivska, joined by Judge Bosnjak

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 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 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 *Barbulescu 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 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 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.

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 Vehabovic

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.

NOOT

---

1. De eerste vraag die het EHRM stelt is of er in dit geval sprake is van een inperking van het recht op privacy, art. 8 EVRM. Als kernvraag stelt het Hof dat beoordeeld moet worden "whether the applicant, or any other individual using the Internet, had a reasonable expectation that his otherwise public online activity would remain anonymous" (par. 98). Interessant is dat het Hof benadrukt dat het gebruik van privacy om illegale handelingen te verrichten niet afdoet aan de reikwijdte van het recht op privacy; ook is er zelden tot nooit verwezen naar de doctrine van misbruik van recht (art. 17 EVRM) in relatie tot art. 8 EVRM. De vraag of art. 8 EVRM van toepassing is, beantwoordt het EHRM aan de hand van drie criteria: (1) 'Nature of the interest involved', (2) 'Whether the applicant was identified by the contested measure' en (3) 'Whether the applicant had a reasonable expectation of privacy'. Waarom het deze drie criteria heeft geselecteerd laat het EHRM zoals gebruikelijk achterwege, wat de rechtszekerheid en de begrijpelijkheid van zijn uitspraak niet ten goede komen.

2. Ten aanzien van het eerste criterium stelt het EHRM dat de naam en identiteit van gebruikers van dynamische IP-adressen niet openbaar zijn (zoals vroeger bijvoorbeeld telefoonnummers, die in een telefoonboek stonden). Wel kan door middel van het IP-adres worden nagegaan welke contacten een persoon heeft gehad en welke informatie hij heeft gedownload en verspreid; dat zegt veel over iemands privéleven en sociale relaties.

3. Ten aanzien van het tweede criterium stelt de overheid zich op het standpunt dat het IP-adres aan de identiteit van de vader was verbonden; toegang tot die gegevens kan dus niet worden gezien als een inperking van de privacy van de zoon. Deze argumentatie verwerpt het EHRM. Door middel van het IP-adres kon de identiteit van de zoon immers worden achterhaald; het doel van het onderzoek was bovendien om de persoon te vervolgen die de strafbare feiten had begaan. Daarvoor was het achterhalen van de identiteit van de eigenaar van de internetverbinding slechts ondersteunend: "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" (par. 112).

4. Ten aanzien van het derde criterium kiest het EHRM een subjectieve benadering en accepteert het "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. 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" (par. 116). Nu de zoon verwachtte anoniem te blijven en anonimiteit een belangrijk onderdeel is van het recht op privacy is *in casu* een inbreuk gemaakt op art. 8 EVRM.

5. Al eerder had het EU Hof van Justitie geoordeeld dat een dynamisch IP-adres een persoonsgegeven kan zijn, in de zin van het recht op gegevensbescherming (*Breyer*, HvJ EU 19 oktober 2016, zaak C-582/14, ECLI:EU:C:2016:779). Het gegevensbeschermingsrecht gaat over het verwerken van persoonsgegevens en een persoonsgegeven is gedefinieerd als 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon' (Algemene Verordening Gegevensbescherming, art. 4.1). Interessant is dat het EU HvJ in zijn oordeel over dynamische IP-adressen benadrukte dat het opslaan van dynamische IP-adressen door bijvoorbeeld websites en platforms als het verwerken van persoonsgegevens moet worden gezien, omdat er wettelijke mogelijkheden bestonden om de naam en het adres van de internetgebruiker te achterhalen. De adressen kunnen als zodanig niemand identificeren, maar zijn wel, in juridisch jargon, 'identificeerbare' gegevens, dat wil zeggen, gegevens die op dit moment nog niemand identificeren, maar in de toekomst mogelijk wel. "Hoewel de verwijzende rechter in zijn verwijzingsbeslissing preciseert dat de internetprovider de extra informatie die noodzakelijk is voor de identificatie van de betrokken persoon, naar Duits recht niet rechtstreeks mag doorgeven aan de aanbieder van onlinemediadiensten, lijken er – onder voorbehoud van de door de verwijzende rechter in dit verband te verrichten verificaties – voor de aanbieder van onlinemediadiensten juridische mogelijkheden te bestaan om zich, met name in geval van cyberaanvallen, te wenden tot de bevoegde autoriteit opdat deze de nodige stappen onderneemt om die informatie van de internetprovider te verkrijgen en om strafvervolging in te stellen. De aanbieder van onlinemediadiensten lijkt dan ook te beschikken over middelen waarvan mag worden aangenomen dat zij redelijkerwijs kunnen worden ingezet om de betrokken persoon met behulp van derden, te weten de bevoegde autoriteit en de internetprovider, te identificeren aan de hand van de bewaarde IP-adressen" (*Bryer*, reeds aangehaald, par. 47-48).

6. In de zaak voor het EHRM gaat het er nu juist om dat er geen wettelijke basis was. Natuurlijk is het zo als de politie door middel van onrechtmatige handelingen toch de identiteit van een verdachte achterhaalt dit niet kan betekenen dat er geen identificeerbare gegevens in het spel zijn. Wel is interessant dat het EHRM bepaalt dat de identificerende gegevens op zich ook

onder het recht op privacy vallen. Het EHRM leunt daarbij sterk op het identificatieprincipe, dat kernonderdeel vormt van het gegevensbeschermingsrecht. Aanvankelijk was het EHRM terughoudend om alles wat onder het recht op gegevensbescherming valt, ook onder de reikwijdte van art. 8 EVRM te laten vallen (B. van der Sloot, *Privacy as virtue*, Intersentia, Cambridge, 2017). Immers, gegevens over personen kunnen wel aan het privéleven en de persoonlijke levenssfeer raken, maar dat hoeft zeker niet. 'Die meneer met de rode muts op' is duidelijk een persoonsgegeven, maar raakt niet direct aan het recht op privacy, zo was de gedachte. Daarom werd het verwerken van publieke en openbare gegevens vaak buiten het recht op privacy geplaatst, wat ook gold voor het verwerken van gewone persoonsgegevens, zoals iemands naam en adres. Steeds meer kiest het EHRM er echter voor om alles wat onder het recht op gegevensbescherming valt ook onder de reikwijdte van art. 8 EVRM te laten vallen (*ibid*). Dat geldt voor publieke gegevens, ongevoelige persoonsgegevens, meta-data en nu dus ook voor de digitale NAW-gegevens (naam, adres, woonplaats).

7. Daarnaast is deze uitspraak van belang omdat het EHRM de 'reasonable expectation of privacy'-doctrine nog sterker omarmt dan voorheen. Het concept van de 'reasonable expectation' is een doctrine die uit de Verenigde Staten is overgewaaid en lange tijd om principiële redenen werd afgewezen in Europa, omdat het een hoogst subjectieve, bewerkelijke en daarmee vage doctrine is. Hoe weet je wat iemands verwachtingen zijn en aan de hand waarvan bepaal je of die verwachting al dan niet redelijk is? De omarming van dit principe staat in een lijn van het EHRM waarin het hoe langer hoe meer vage bepalingen aan zijn begrippenkader toevoegt, zoals 'the quality of life', 'the quality of the law', 'chilling effect', 'pressing social need' en 'balancing' (zie daarover onder andere: B. van der Sloot, 'Ten questions about balancing', *European Data Protection Law Review*, 2017-2). Door vage en subjectieve concepten te gebruiken kan het EHRM steeds meer macht naar zich toetrekken, aangezien hij uiteindelijk besluit of een verwachting redelijk is, of de wet kwalitatief goed gemaakt is, hoe een balans tussen twee rechten moet uitvallen, etc. (wat telkens *in ultimum* een subjectieve keuze is). Ook wordt daarmee de rechtszekerheid steeds minder. Het is bijvoorbeeld van te voren niet goed te voorspellen hoe een belangenafweging tussen twee rechten zal uitvallen, omdat rechten geen gewicht hebben en er geen juridische weegschaal bestaat met objectieve criteria om een gewicht te meten en te wegen. Balanceren is uiteindelijk een subjectieve exercitie die van geval tot geval anders kan uitvallen, afhankelijk van de gevoelens en overtuigingen van de rechter.

8. Dat blijkt ook uit de *concurring opinion* van rechter Yudkivska, waarbij rechter Bosnjak zich heeft aangesloten, die een nogal liberale inborst heeft, onder meer uit het werk van Ayan Rand citeert en meent dat we in een politiestaat leven. Hij meent dat het EHRM nog duidelijker had moeten maken dat het aftappen van data, communicatiedata en metadata een grove schending is van de privacy en een stap naar een totalitaire samenleving betekent. Uit de *dissenting opinion* van rechter Vehabovic volgt juist weer een tegenovergesteld standpunt, hij meent dat er geen schending van de privacy was, aangezien het IP-adres naar de identiteit van de vader leidde en niet naar die van de zoon. "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 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" (*dissenting opinion*).

9. Daarbij komt dat bij de ‘reasonable expectation of privacy’ het niet alleen de vraag is hoe nu moet worden beoordeeld wat de verwachting van een persoon was en of die redelijk was, maar ook dat daarmee het gevaar is, dat als privacyschendingen steeds openlijker worden gepleegd en steeds meer een standaardonderdeel van de samenleving worden (*mass surveillance, predictive policing, data retention* etc.), het wellicht niet meer redelijk wordt om te verwachten dat burgers ten aanzien van dergelijke praktijken privacy hebben. Zo is in de Verenigde Staten onder meer de ‘third party doctrine’ ontwikkeld, waaruit volgt dat als een persoon zijn informatie deelt met één persoon of instantie, hij ook geen redelijke verwachting meer heeft dat die persoon of instantie die informatie niet door zal geven aan derden. Ook IP-adressen vallen in de Verenigde Staten onder de *third party doctrine*. Het is dus maar de vraag hoe wenselijk het is om ook de doctrine van de *reasonable expectation of privacy* in Europa te omarmen. Ook valt op dat deze term wel uit het Amerikaanse recht wordt gehaald, maar de bijbehorende *third party doctrine* niet; hoe dat precies moet worden begrepen blijft onduidelijk.

10. Nu door het EHRM is vastgesteld dat er een inbreuk op de privacy is geweest, is de tweede vraag of de inbreuk was voorgeschreven bij wet. Die vraag beantwoordt het Hof negatief, waarbij het verwijst naar een aantal feiten. Er was geen duidelijke wettelijke basis voor de toegang tot de data voor de politie; de wettelijke bepaling was vaag en het was niet redelijk te voorzien voor de klager dat de regeling op deze wijze zou worden geïnterpreteerd. Er was ook geen rechterlijk bevel voor het verzamelen van de data door de politie en tot slot was ook de ‘quality of law’ niet gewaarborgd, dat wil zeggen dat er onvoldoende waarborgen waren tegen misbruik van bevoegdheden door de politie: “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” (par. 130). Derhalve is er een schending van art. 8 EVRM.

dr. B. van der Sloot, Senior Researcher, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University

VOETNOTEN

1Ayn Rand, The Fountainhead.

2See 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.

3Ibid., pp. 20 and 22.

4Warren & Brandeis, the Right to Privacy, 4 HARV. L. REV. 193 (1890).

5Osborn v. United States, 385 U.S. 323 (1966).

6Katz v. United States, 389 U.S. 347 (1967).

7*Halford v. the United Kingdom*, 25 June 1997, *Reports of Judgments and Decisions* 1997 III.

8*Copland v. the United Kingdom*, no. 62617/00, ECHR 2007-I.

9GC, no. 61496/08, ECHR 2017 (extracts).

10Smith v. Maryland, 442 U.S. 735 (1979).

11See 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.

12United States v. Heckenkamp, 482 F.3d 1 142, 1 146 (9th Cir. 2007).

13United States v. Howe, 2011 WL 2160472 at. 7 (W.D.N .Y. May 27, 2011).

14State v. Reid, 945 A.2d 26, 28 (N.J. 2008).

15The 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).

16PACE Resolution on Mass Surveillance 2045 (21 April 2015).

17*Malone v. the United Kingdom*, 2 August 1984, Series A no. 82.

18UN 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).

19Bruce Schneier, “Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World”, New York, N.Y.: W.W. Norton & Company, 2015.