THE PROTECTION OF PRIVACY OF THE IP ADDRESS IN SLOVENIA

Matija Damjan*

ABSTRACT

The protection of communication privacy covers not only the content of the conversation, but also other information related to the communication (metadata). The most prominent type of metadata in online communication is IP address, which defines the location of a computer or other connected device in the network. As a purely technical information, an IP address does not refer directly to any individual and is not in itself personal information. Yet, it can also be used to identify individuals online, track their location and online activity. An IP address is never strictly private, since any internet user's IP address is visible to other participants in regular online interactions, which differentiates it from typical private information. The paper examines the conditions, developed in case law of the European Court of Human Rights and Court of Justice of the European Union as well as the Slovenian courts, under which an IP address can be considered personal data and when it is protected as a part of one's communication privacy. The paper then focuses on the issue of whether an individual should be considered to have waived the privacy protection of their IP address if they have taken no measures to hide it. The relevance of the distinction between static and dynamic IP addresses from the perspective of privacy protection is also discussed.

KEYWORDS

IP address
metadata
internet
communication privacy
data protection

* | Assistant Professor, University of Ljubljana, Faculty of Law, and Secretary General, Institute for Comparative Law at the Faculty of Law, Slovenia, matija.damjan@pf.uni-lj.si, ORCID: 0000-0001-6063-0328.

https://doi.org/10.55073/2022.2.25-43

1. Introduction

Browsing of the web and other online activities may appear anonymous to the average Internet user, yet this is an illusion. Any computer or other device connected to the Internet is assigned a numerical identifier called an IP address (Internet Protocol Address), which defines the location of the device in the network and is visible to other devices. The internet service provider (ISP) may keep logs of websites visited by their IP addresses, and the website owners may record the IP addresses of their visitors. Although an IP address does not directly reveal the user of an Internet-connected device, it can be used to track the user's location and Internet activity. An ISP can also match IP addresses with concrete subscribers of its services, thus identifying the Internet users.[1] As a link between the physical and virtual worlds, an IP address is also an almost inevitable first step in investigating online crime.[2]

The manner of protection of the IP address as a part of the individuals' private sphere is not expressly regulated either in the Slovenian or in the EU's legislation, so the answer depends on the interpretation of the relevant statutory provisions by the courts and other competent authorities. An IP address can be viewed and legally protected either as personal data or metadata related to private online communication. The distinction between the two is particularly relevant from the perspective of Slovenian law, which has established specific procedural safeguards for the protection of communication privacy. Although several judicial decisions have been made, the issue is far from settled, and opposing views are advocated in the legal literature.[3] Due to different contexts in which an IP address can appear, a uniform answer seems unlikely.

The paper will focus on the question of whether and under what conditions an IP address is legally protected as private. We will first examine its protection under the rules of data protection (information privacy) and then under the scope of communication privacy rights. Both aspects of privacy are protected under the Constitution of the Republic of Slovenia,[4] as well as the European Convention on Human Rights (ECHR)[5] and the Charter of Fundamental Rights of the European Union (EUCFR).[6] All three legal acts are directly applicable to the Slovenian legal system and take precedence before ordinary legislation; therefore, they must be read and interpreted in conjunction.

An overview of the relevant provisions will be followed by an analysis of the leading decisions of the highest Slovenian courts as well as the Court of Justice of

1 | Daly, 2022, p. 198.
2 | Golobinek, 2021, p. II.
3 | For example, the discussion between Zagozda and Lesjak for and against the protection of IP address as personal data. Zagozda, 2022, pp. 10–11; Lesjak, 2022, pp. 14–15.
4 | Official Gazette of the Republic of Slovenia, No. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06, 47/13 and 75/16.
5 | Convention for the Protection of Human Rights and Fundamental Freedoms, ETS no. 005, adopted in Rome on 4. 1. 1950.
6 | OJ C 326, 26. 10. 2012, pp. 391–407.

the European Union (CJEU) and the European Court of Human Rights (ECtHR) on this issue. The paper will then focus on whether an individual should be considered to have waived the privacy protection of their IP address if they have taken no measures to hide it. This aspect will be examined through the Benedik case[7] decided before Slovenian courts and the ECtHR. The relevance of the distinction between static and dynamic IP addresses from the perspective of privacy protection is also discussed.

2. Privacy implications of IP addresses

An IP address is a unique series of digits assigned to every device on a network, which allows the devices to recognize and communicate with each other using the Internet Protocol.[8] When a website is accessed, the IP address of the computer seeking access is communicated to the server on which the consulted website is stored. This connection is necessary so that the data accessed may be transferred to the correct recipient. Therefore, the IP address of any Internet-connected device must be visible to other participants in online interactions. An IP address can either be static or dynamic. A static IP address is permanently allocated by the ISP to a particular device. A dynamic IP address, however, is temporarily assigned to a device by the ISP, typically each time the device connects to the Internet, and is replaced when subsequent connections are made. Most dynamic IP addresses can only be traced to the ISP to which the user is connected and not to a specific computer. Normally, only the ISP has knowledge of the IP addresses used by its customers.[9]

An IP address in itself is purely technical information that enables communication between Internet-connected devices. Under Internet Protocol Version 6 (IPv6), IP addresses consist of 128 bits and are written as eight four-digit hexadecimal numbers separated by colons.[10] The series of digits does not contain any personal data and is not directly linked to any individual, but only refers to a specific device in the network. The first two sets of quads are used to identify the network location of the device. This can show the geolocation of the device and, indirectly reveal its user. However, because most users are connected to the network through an ISP and use a router, their IP address reveals only the general geographic area from which the information was sent, whereas the user's exact geographic address is only known to their ISP.[11]

7 | ECtHR case Benedik v. Slovenia, no. 62357/14, 24. 4. 2018.
8 | The end-to-end data communication on the internet is based on a set of communication protocols commonly known as the TCP/IP. The Transmission Control Protocol (TCP) breaks the data into packets ready for transmission and recombines them on the receiving end. The Internet Protocol (IP) handles the addressing and routing of the data and delivers packets from the source host to the destination host solely based on the IP addresses in the packet headers. Murray, 2010, p. 23.
9 | Daly, 2022, p. 198.
10 | Murray, 2010, p. 24.
11 | Ibidem.

Although an IP address does not directly reveal its user's identity, it can be used to track a person's online behavior by those who know which IP address is used by which individual, for example, their employer (for work computers), their ISP or mobile service provider, or the law enforcement authorities that have obtained the information on the identity of the user of an IP address from the ISP. Most websites routinely record visitors' IP addresses. By combining the collected information on website visits, one can construct profiles of Internet users to extract their professional, consumer, sports, political, religious, and sexual interests and preferences. In fact, the EU's Data Retention Directive[12] required ISPs to retain for a limited time the name and address of the subscriber or registered user to whom an IP address, user ID, or telephone number was allocated at the time of the communication, which mandated a sort of blanket passive surveillance.[13] However, in 2014, the CJEU declared the Directive invalid on the grounds that blanket data collection violated the fundamental rights to privacy and data protection enshrined in the EUCFR.[14]

Users who are concerned about online privacy can adopt technological measures to protect themselves from the risks of surveillance or misuse. For example, a Virtual Private Network (VPN) service, which allows users to connect to the Internet through encrypted tunnels that do not reveal their true IP address, can be used. Another option is the use of an anonymous browser, such as Tor, which actively conceals the user's identity by accessing websites through several consecutive IP addresses that keep changing (onion routing).[15]

Apart from such technological solutions, however, the privacy of one's IP address is also protected by legal means. Owing to the nature and function of IP addresses, two avenues of legal protection are available: data protection rules and provisions guaranteeing communication privacy.

3. IP address as personal data

3.1. Legal bases

In Slovenian constitutional law, data protection is usually understood as an aspect of the general right to privacy, as stated in Article 35 of the Constitution. This is why it is also referred to as information privacy.[16] Article 38 of the Slovenian Constitution specifically guarantees the protection of personal data and prohibits the use of personal data contrary to the purpose for which it was collected. Everyone has the right to access the collected personal data that relates to them and the

12 | Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54–63.
13 | Murray, 2010, p. 519.
14 | Joined Cases C-293/12 and C-594/12 Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Others, 8. 4. 2014. See Brkan, 2019, p. 871.
15 | Zagozda, 2022, p. 11.
16 | Cerar, 2009, p. 1409; Brkan, 2014, p. 70.

right to judicial protection in the event of any abuse of such data. The Constitution mandates that the collection, processing, designated use, supervision, and protection of the confidentiality of personal data be regulated by law.

Under the ECHR, the origin of the right to data protection lies in the right to privacy. The Convention does not mention personal data and only speaks of the protection of private and family life,[17] but under the established case law of the ECtHR,[18] storage of information relating to an individual's private life and the release of such information is also considered to be governed by this provision. To fall within the scope of Article 8, the information or data in question must be private in the sense that it is confidential.[19] In the Council of Europe's law, the term personal data is defined in Article 2 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[20] as any information relating to an identified or identifiable individual (data subject).

European Union law distinguishes more clearly between the right to privacy and the right to data protection, and both are specifically regulated. The respect for private and family life is guaranteed in Article 7 of the EUCFR, whereas Article 8 guarantees the protection of personal data, provided that such data is processed fairly for specified purposes, and is based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access data that has been collected concerning them and the right to have it rectified. Legal theory points out that the right to data protection intends to protect interests that underlie the right to privacy, as well as other fundamental rights, such as the right to non-discrimination. Hence, both rights under the EUCFR are closely connected but separate.[21] In the Bavarian Lager case, the Court of First Instance stressed that a disclosure of personal data does not in itself also constitute a breach of the right to privacy, as not all personal data are by their nature capable of undermining the private life of individuals.[22]

The EU's data protection rules are contained in the General Data Protection Regulation (GDPR).[23] Under Article 4(1) of the GDPR, personal data refers to any information relating to an identified or identifiable natural person (data subject), whereas an identifiable natural person is 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, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. An almost identical and certainly equivalent definition of personal data was contained in Article 2(a) of the Data Protection

17 | Article 8 of ECHR.
18 | E.g., case M.M. v. the United Kingdom, no. 24029/07, 13. 11. 2012.
19 | Schabas, 2015, p. 383.
20 | ETS no. 108, adopted in Strasbourg on 28. 1. 1981.
21 | Kranenborg, 2021, pp. 237–239; Brkan, 2014, p. 70.
22 | Case T-194/04 Bavarian Lager v Commission, 8. 11. 2007, paras. 118–119.
23 | 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, OJ L 119, 4.5.2016, pp. 1–88.

Directive,[24] which was applicable before the GDPR, so that the case law and legal theory developed under the Data Protection Directive concerning the definition of personal data still hold true under the GPDR.[25]

The definition of personal data is of vital importance for determining whether the GDPR applies and for the general application of data protection laws.[26] Data that are not personal are usually referred to as anonymous data.[27] If an IP address is to be treated as personal data, then all the obligations under the GDPR concerning the processing of personal data apply. This means that for the processing to be lawful, it can only be performed on the basis of the consent of the data subject concerned or some other legitimate basis laid down by law.[28] Hence, the legal qualification of IP addresses is essential to determine the scope of obligations of ISPs and online service providers, as well as law enforcement authorities investigating online crime.

The GDPR does not expressly answer whether IP addresses are personal data. However, online identifiers are mentioned as an example in its definition of personal data. Recital 30 explains that natural persons may be associated with online identifiers provided by their devices, applications, tools, and protocols, such as IP addresses, cookie identifiers, or other identifiers such as RFID tags. This may leave traces that, in particular, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.[29] Online identifiers are non-personal metadata that contain information about other data that could be personal.[30]

3.2. CJEU case law

The CJEU first considered the question of whether an IP address can constitute personal data in the Scarlet Extended case [31] in 2011. The Court simply held that IP addresses are protected personal data because they allow users to be precisely identified.[32] No further analysis or explanation of the conditions of identification was provided, but considering the circumstances of the case, it was possible to conclude that an IP address is a piece of personal data when in the hands of an ISP that provides internet access to the relevant individual, assigns them the IP

24 | 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 L 281, 23.11.1995, pp. 31–50.
25 | Zuiderveen Borgesius, 2017, p. 137.
26 | The definition of personal data is usually broken down into four constituent elements: (1) information (2) relating to (3) identified or identifiable (4) natural person. Bygrave and Tosoni, 2020, p. 109.
27 | Ibidem, p. 105.
28 | Article 6 of the GDPR.
29 | Lesjak, 2022, p. 14.
30 | El Khouri, 2017, p. 195.
31 | Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs (SABAM), 24. 11. 2011.
32 | Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs (SABAM), 24. 11. 2011, para. 51.

address, and keeps a record of this allocation.[33] Hence, the CJEU did not consider the status of IP addresses alone, separate from other information that allows an ISP to quickly identify users of specific IP addresses.

The Digital Rights Ireland case of 2014, which invalidated the Data Retention Directive, did not add further reasoning in this regard. However, it seems likely that the CJEU was concerned about the combination of IP addresses with content and subscriber information, which clearly meant that the stored data could be used to identify individuals.[34]

The Court defined the circumstances in which IP addresses constitute personal data in more general terms in the Breyer case[35] in 2016. The case involved several websites operated by German federal institutions to provide general topical information to the public. To prevent denial-of-service attacks (DDoS), the sites store information on all access operations in log files. The information stored included the name of the website, search terms entered, time of access, quantity of data transferred, an indication of whether the access was successful, and the IP address of the computer that accessed the website. Patrick Breyer sued the German federal government, seeking an order to restrain the government from storing access information relating to his visit to the website. Breyer claimed that IP addresses qualify as personal data and that the government therefore required express consent from individuals concerned to process such data. The Administrative Court dismissed Breyer's action, whereas the Court of Appeal granted the injunction in part. It held that IP addresses constitute personal data only where the Internet users reveal their identity to the website operator. While only the user's ISP can identify the user of a dynamic IP address through their account details, the IP address does not amount to personal data in the hands of a website operator. The case reached the German Federal Court of Justice, which referred the issue to the CJEU.

In its judgment, the CJEU first noted that it had held IP addresses to be personal data in Scarlet Extended but pointed out that the finding concerned a situation in which the collection and identification of IP addresses of Internet users was to be carried out by ISPs who could directly identify their customers from their IP addresses. Under the definition of the Data Protection Directive, personal data must allow data subjects to be identified directly or indirectly.[36] The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that the information alone allows the data subject to be identified.[37] The CJEU then turned to Recital 26 of the Data Protection Directive which stated that 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.' In the Court's reading, this wording suggested that for information to be treated as personal data, it is not required that

33 | Zuiderveen Borgesius, 2017, p. 134.
34 | Stalla-Bourdillo and Knight, 2016, p. 315.
35 | Case C-582/14 Patrick Breyer v Germany, 19. 10. 2016.
36 | Ibidem, para. 33.
37 | Ibidem, para. 41.

all the information enabling the identification of the data subject be in the hands of one person. However, it must be determined whether the possibility of combining a dynamic IP address with the additional data held by the ISP constitutes a means that is likely reasonably to be used to identify the data subject. This would not be the case if the identification of the data subject was prohibited by law or practically impossible due to a disproportionate effort required.[38] Although the referring court stated that German law does not allow ISPs to transmit data necessary for the identification of a data subject directly to online media service providers, the CJEU pointed out that in the event of cyber-attacks, legal channels exist for the service provider to contact a competent authority so that the latter can obtain that information from the ISP and bring criminal proceedings. The CJEU concluded that online media services provider has the means which may likely reasonably be used to identify the data subject on the basis of the IP addresses stored, with the assistance of the competent authority and the ISP.[39]

The CJEU adopted a relative criterion under which a dynamic IP address constitutes personal data in the hands of any party that either has or can lawfully obtain sufficient additional data from a third party to link the IP address to a specific person's identity.[40] Even where the possibility of obtaining such identifying information exists only subject to specific conditions laid down in law, this is sufficient to render the IP address personal data as long as this channel is reasonably likely to be used in the identification process.[41] However, the same IP address will not be considered personal data when in the hands of a party that has no legal means of obtaining sufficient additional data to make such a link.

3.3. Position of the Slovenian Information Commissioner

The Slovenian Information Commissioner has long held in its advisory opinions that IP addresses should be considered personal data in most situations because they can be used, at least indirectly, to identify individuals. The earliest such opinion was issued in 2006 and likened an IP address to an individual's mobile telephone number, as they both refer to individuals and can be used to identify them.[42] By 2010, the Information Commissioner had developed the position that a dynamic IP address is considered personal data when combined with information on the time it was assigned or the time of access to the network, whereas a static IP address is always considered personal data because the individual user is always identifiable. In the Information Commissioner's opinion, the publication of IP addresses of users of an online service on a website is permissible only if they voluntarily agree to such

38 | Ibidem, paras. 44–45.
39 | Ibidem, paras. 48–49.
40 | Zuiderveen Borgesius, 2017, p. 135. This position was confirmed in the CJEU's subsequent case law, e.g. in case C-597/19 Mircom International Content Management & Consulting v Telenet, para. 102.
41 | Bygrave and Tosoni, 2020, p. 111. El Khouri points out that under the same logic and metadata and, in fact, any information could potentially be personal data. The risk of identification increases with the number of databases and possible correlations that can be made. El Khouri, 2017, p. 196.
42 | 092-4/2006/359, 22. 6. 2006.

processing of their personal data. Permission can also be given tacitly, by posting an online comment where the rules of the online newspaper require the publication of the commenter's IP address together with their comment.[43]

The Information Commissioner's interpretation of IP addresses as personal data seems to have remained unchanged after the entry into force of the GDPR. In a recent opinion, the commissioner stated that an IP number is a unique number with which each computer is identified in the network as an address. With its help, the individual user is identified or at least identifiable. Accordingly, the IP address is personal data, which means that an employer needs an appropriate legal basis for processing employees' IP addresses.[44]

The Information Commissioner's position on IP addresses as personal data has not been expressly confirmed in judicial proceedings, as the courts tend to deal with the protection of individuals' IP addresses within the context of communication privacy rather than data protection. Therefore, even in cases where the Information Commissioner's opinions on this issue were involved in the proceedings, the courts tended to avoid giving a direct answer to the question.[45] The Supreme Court came close to the CJEU's later reasoning in Breyer in a criminal case decided in 2016. It held that an IP address, as purely technical data, did not in itself enable the identification of the convict who could only be identified by using additional information available to the operator of the online network.[46] Again, the reasoning behind the decision was grounded in the right to communication privacy rather than data protection.

4. Communication privacy and metadata

4.1. Legal bases

An IP address is the technical information required to establish any online communication. It is separate from the content of the communication, yet closely related to it as metadata. As such, it can also be protected under the fundamental right to communication privacy, which is guaranteed in Article 37 of the Slovenian Constitution, as well as in Article 8 of the ECHR and Article 7 of the EUCFR. The provision on communication privacy in Article 37 of the Constitution expressly refers only to letters and correspondence. Nevertheless, it is clear in the Constitutional Court's case law that the Constitution protects the privacy of any mode of communication.[47] Regardless of the technology used, protection extends to any communication that is not public and about which a person can reasonably expect privacy.[48] The same applies to the ECtHR's case law concerning the interpretation

43 | 0712-2/2010/2277, 24. 12. 2010.
44 | 07121-1/2021/1379, 4. 8. 2021.
45 | See, for example, judgment of the Administrative Court I U 1079/2012, 14. 5. 2014, and its decision I U 964/2014, 30. 6. 2014.
46 | Judgment I Ips 27119/2014, 17. 11. 2016. See Križnar, 2017, pp. 17–18.
47 | Decision Up-106/05, 2. 10. 2008.
48 | Klemenčič, 2011, pp. 530–531.

of the term correspondence in Article 8 of the ECHR.[49] As the most recent of the three documents, the EUCFR uses the term communications instead of correspondence in Article 7 to precisely account for technological developments. The protection of communication includes not only correspondence of personal or intimately private nature between natural persons but also correspondence with professional and commercial content.[50]

The Slovenian Constitution lays down stricter procedural safeguards for communication privacy than the constitutions of most other European countries: a court order is needed for any interference with the right to a person's communication privacy, and such a court order can only be issued when expressly provided for by law (adopted by the National Assembly) if such interference is necessary for the institution or course of criminal proceedings or for reasons of national security.[51] The higher threshold of constitutional protection of communication privacy is based on the fact that remote communication is conducted via the post office, telecommunication, or computer network, over which the sender has no direct control. Hence, communication is more vulnerable to interference by the state or uninvited third parties rather than other spheres of privacy.[52]

Unlike in the field of data protection, no secondary legislative act defines the exact extent of communication privacy in general. Therefore, there is no express provision specifying the conditions under which an IP address should be considered legally protected private information. However, the e-Privacy Directive[53] is relevant in this regard, as it requires Member States to ensure the confidentiality of communications made over public networks. IP addresses are encompassed by the term 'traffic data', which is defined as any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.[54] Member States must prohibit any type of surveillance or interception of communications and traffic data without the consent of users, except if the person is legally authorized and in compliance with specific requirements. They must also guarantee that access to such information stored on the user's personal equipment is only permitted if the user has been clearly and fully informed, among other things, of the purpose and has been given the right of refusal.[55] When traffic data are no longer required for communication or billing, they must be erased or made anonymous unless the service provider has the users' consent to use these data for marketing purposes.[56]

49 | Schabas, 2015, p. 400.
50 | Mangan, 2021, p. 161.
51 | Pirc Musar, 2018, p. 559.
52 | Klemenčič, 2011, p. 530.
53 | Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37–47.
54 | Article 2(b) of the Directive on privacy and electronic communications.
55 | Article 5 of the Directive on privacy and electronic communications.
56 | Article 6 of the Directive on privacy and electronic communications.

The requirements of the e-Privacy Directive have been transposed into Slovenian law under the Electronic Communications Act (ZEKom-1),[57] which also contained provisions[58] requiring mandatory retention of traffic data by the ISPs, including the users' IP addresses, in line with the Data Retention Directive. However, following the invalidation of the Directive by the CJEU in the Digital Rights Ireland case, the Slovenian Constitutional Court also invalidated these provisions of ZEKom-1 as unconstitutional. The review of constitutionality was initiated upon the request of the Information Commissioner, who argued that the precautionary retention of data entailed inadmissible interference with the rights to the protection of personal data as well as communication privacy.[59] Interestingly, the Constitutional Court satisfied itself with the finding that the measure disproportionally interfered with the right to the protection of personal data. Since the challenged provisions had to be abrogated due to this conclusion, the Constitutional Court did not assess the other alleged unconstitutionalities[60] and thus avoided an express statement as to when an IP address could be protected under the right to communication privacy.

4.2. Case law

In 2008, the Constitutional Court clarified that the protection of communication privacy is not limited to the content of communication but extends to traffic data that relate to it (data on the manner and parties to the communication, such as timing, duration, and geolocation).[61] The case concerned a criminal investigation of a legally seized mobile phone and SIM card. The complainant, who had been convicted based on the list of telephone numbers and text messages obtained from his SIM card, claimed that this evidence was unlawful, as the police had monitored his mobile telephone communication without a court order. The Constitutional Court upheld the complaint, stating that the protection of communication privacy also includes any data on telephone calls, which are an integral part of communication. It held that the traffic data obtained from the printout of the telephone memory should be considered an integral part of communication privacy. Accordingly, accessing the information on the last-made calls and last-missed calls, as well as examining the content of SMS messages stored on the phone, were held to be intrusions into the communication privacy for which a court order is required.

Although the Constitutional Court's decision concerned traffic data related to phone calls, the same reasoning applies to traffic data related to any kind of communication. Therefore, IP addresses must also fall within the scope of communication privacy under Slovenian law.[62] This position was expressly adopted by the Information Commissioner in several advisory opinions, which explained that information on the IP address from which an individual communicated belongs to

57 | Official Gazette of the Republic of Slovenia, No. 109/12, 110/13, 40/14, 54/14, 81/15, 40/17 and 189/21.
58 | Articles 162–169 of ZEKom-1.
59 | Articles 37 and 38 of the Constitution.
60 | Case U-I-65/13, 3. 7. 2014, paras. 27–29.
61 | Decision Up-106/05, 2. 10. 2008.
62 | Klemenčič, 2011, p. 522; Lesjak, 2019, p. 357.

the traffic data, and as part of the communication, enjoys protection under Article 37 of the Constitution. Therefore, an IP address should only be obtained by the police based on a court order.[63]

Ordinary courts have followed the same reasoning in criminal procedures, so evidence obtained by the police based on the defendant's IP address that was not acquired through a court order is usually held inadmissible due to the violation of the fundamental right to privacy.[64] However, the Appellate Court in Ljubljana developed a doctrine in which dynamic IP addresses enjoy a higher level of protection than static IP addresses. The reasoning behind this distinction will be discussed in Subchapter 5.

4.3. What constitutes a waiver of IP address privacy?

Slovenian courts have held in a number of cases that Internet users have waived the privacy of their IP address by exposing it somehow through their online activities. In such situations, the IP address did not enjoy protection under the scope of communication privacy rights, as it was no longer private. Accordingly, the courts held that IP addresses did not enjoy protection under the scope of communication privacy rights in several criminal cases where the defendants had been using a peer-to-peer (P2P) file sharing network in which all users of the network were able to see the IP addresses of other users, but not their identities.[65] Similarly, posting an offensive comment on a public online forum was held by the Supreme Court as public communication, in connection with which an individual could not expect communication privacy, even when their IP address is concerned.[66]

However, the final position on the waiver of the IP address privacy issue was developed in the Benedik case that was decided by the courts at all levels, up to the ECtHR. Mr. Benedik, who was sentenced for possessing and distributing child pornographic material, had been identified by the Slovenian police on the basis of the IP address assigned to his computer. The IP address was obtained by the Swiss police simply by monitoring the P2P file-sharing network Razorback, in which any user of the site could review the IP addresses of all other users uploading or downloading files. Without obtaining a court order, the Slovenian police requested a Slovenian ISP to disclose data regarding the user to whom the IP address had been assigned. During the house search, the police found that one of the seized computers contained files with pornographic material involving minors. Benedik was convicted, and both the Court of Appeals and the Supreme Court rejected the allegation of illegally obtained evidence.[67] The Supreme Court reasoned that the communication in question could not be considered private since the Swiss police could check the exchanges in the P2P network without any intervention in Internet traffic, simply by monitoring the users' sharing activity. Moreover, in the Supreme

63 | Advisory opinions 0712-1/2012/2854, 4. 6. 2013, 0712-1/2014/711, 20. 2. 2014 and 0712-1/2014/1651, 17. 4. 2014.
64 | Decision of the Appellate Court in Maribor II Kp 50396/2011, 9. 10. 2018.
65 | Judgment of the Supreme Court of Slovenia I Ips 216/2010, 20. 1. 2011; decision of the Appellate Court in Celje III Kp 53999/2011, 21. 4. 2015.
66 | Judgment of the Supreme Court of Slovenia I Ips 27119/2014, 17. 11. 2016.
67 | Golobinek, 2021, p. II.

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 computer through which the Internet had been accessed.[68]

The Constitutional Court rejected Benedik's constitutional complaint.[69] While the Court acknowledged that the right to communication privacy under Article 37 of the Constitution also protects traffic data, including IP addresses, it concluded that Benedik had consciously exposed his IP address to the public by using a public P2P network in which his IP address was not in any way hidden. Hence, he could not legitimately have expected privacy and his IP address was not protected under communication privacy under Article 37 of the Constitution but only as personal data under Article 38 of the Constitution. This allowed the police to obtain data regarding the identity of the dynamic IP address user from the operator without a court order.[70]

Benedik lodged an application before the ECtHR claiming the violation of his privacy rights under Article 8 of the ECHR.[71] The ECtHR followed the assessment of the Slovenian Constitutional Court that privacy rights also refer to obtaining data on the user of a (dynamic) IP address for criminal proceedings. Contrary to the Constitutional Court, however, the ECtHR held that the complainant had not waived the expected privacy online by failing to take measures to hide his dynamic IP address. In ECtHR's view, the question was 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. The ECtHR did not overlook the fact that revealing the identity of the IP address user also discloses other intimate details of the individual's life, which are evident from his Internet activity. The complainant never disclosed his identity in relation to the online activity in question, nor was it identifiable by the service provider through an account or contact data. Therefore, the ECtHR concluded that such an online activity engaged a high degree of anonymity as 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.

The ECtHR also noted that at the relevant time, no regulation specified the conditions for the retention of communication data obtained in criminal investigations and there were no safeguards against abuse by state officials in the procedure for access to and transfer of such data. The police, with information on a particular online activity at their disposal, could have identified an author by merely asking the ISP to look up that information. Furthermore, no independent supervision of

68 | Pirc Musar, 2018, p. 555.

69 | Decision of the Constitutional Court of Slovenia Up-540/11, 13. 2. 2014.

70 | Pirc Musar, 2018, pp. 555–556; Križnar, 2018, pp. 6–7. The Information Commissioner did not follow the Constitutional Court's position and continued to issue opinions that the IP address is a traffic data that does not on its own reveal its user's identity. Therefore, the user does not give away their anonymity simply by providing the IP address to the public. See opinions 0712-1/2014/1651, 17. 4. 2014, 0712-1/2014/3025, 25. 9. 2014, and 0712-1/2017/130, 24. 1. 2017.

71 | ECtHR case Benedik v. Slovenia, no. 62357/14, 24. 4. 2018.

the use of these police powers was shown to exist at the relevant time. The ECtHR therefore found a violation of Article 8 of the ECHR, which protects privacy.[72] The most important part of the judgment might be the clear and unambiguous statement that an IP address is an integral part of not only information privacy but also communication privacy.[73]

In its action report, Slovenia informed the Council of Europe that the Criminal Procedure Act[74] had been amended accordingly following the ECtHR ruling, so that it now clearly states that a court order is required to obtain traffic data as well as to obtain subscription data where the processing of traffic data is required.[75] Slovenian courts also gave full effect to the ECtHR's judgment. The Supreme Court overturned Benedik's conviction,[76] explaining that the technical anonymity of IP addresses justifies users' legitimate expectation that their online activity will be private. Even if a user of a P2P network cannot expect privacy regarding their IP address, which is visible to other users of the network, this does not mean that they have revealed their identity. To determine whether a person has waived their privacy with regard to their identity, the court must examine whether they have disclosed their personal data in connection with the online activity so that the police can access the same based on a review of publicly available data. Otherwise, the IP address is also protected in the context of communication privacy and not only in the context of information privacy.

The Constitutional Court cited the ECtHR's decision in the Benedik case in another case[77] in which the complainant, who had published an offensive comment on an online forum, was identified through her IP address obtained by the injured party's attorney from the provider of the online forum. The appellant challenged the judgment of the District Court, which found her guilty of defamation. The Constitutional Court acknowledged that the complainant had deliberately disclosed the content of her communication to the public (i.e., the content of the disputed comment), as she wrote the comment under the article on the web portal, and any visitor to the article could access the article and comments below it. However, the comment was published anonymously (under the username 'guest-citizen') and the author's IP address or any other identifying information were not revealed on the website. Therefore, in the Court's view, it could not be argued that the complainant deliberately exposed her IP address to the public through public communication or that she thereby disclosed her identity and knowingly waived her expectation of privacy. Consequently, the dynamic IP address was the subject of the protection of communication privacy under Article 37 of the Constitution, and the acquisition of an IP address in this case constituted interference with this human right.

72 | Golobinek, 2021, p. IV.
73 | Pirc Musar, 2018, p. 560; Križnar, 2018, pp. 7–8.
74 | Official Gazette of Republic of Slovenia, no. 176/21 and 96/22.
75 | Communication from Slovenia concerning the case of Benedik v. Slovenia (Application No. 62357/14) Revised Action Report (06/10/2021), pts. 15–20.
76 | Judgment of the Supreme Court of Slovenia I Ips 31751/2018, 4. 6. 2020.
77 | Up-153/17, 9. 9. 2021.

5. Static IP addresses

The technical difference between dynamic and static IP addresses seems relevant in the context of both personal data protection and communication privacy. However, the precise legal consequences of this distinction remain unclear. Both, the Breyer and Benedik cases only concerned dynamic IP addresses, and neither the CJEU nor the ECtHR have stated the extent to which their findings also concern static IP addresses. Interestingly, the potential consequence of these technical differences is that static IP addresses can be protected more strictly than dynamic IP addresses under data protection rules, whereas the result would be the opposite in the field of communication privacy.

As static IP addresses remain unchanged for longer periods, a website operator has a better chance of recognizing returning visitors over a longer period based on their IP address in combination with some additional information derived from their online activity that could link the address to a specific individual. In terms of the Breyer criteria, the longer the same static IP address is used, the greater the likelihood that sufficient additional data will accumulate that could be used to identify the user of the IP address. Therefore, in general, a static IP address should sooner be regarded as a piece of personal data than a dynamic IP address.[78]

In the field of communication privacy, the crucial circumstance is that a static IP address is assigned to the party at its request, and the ISP maintains a directory of assigned and free IP addresses, from which it can directly extract information about the subscriber to whom the static IP address has been assigned. The Criminal Procedure Act does not require a court order for the police to obtain subscriber data from the ISP if no traffic data processing is required. On this basis, the Appellate Court in Ljubljana developed a distinction between the privacy status of dynamic and static IP addresses. It held that each attempt to access the Internet via a dynamic IP address creates traffic data that must be processed to identify the user. Since traffic data are an integral part of communication, identifying the user of a dynamic IP address always falls within the scope of protection of communication privacy. To identify the user of a static IP address, however, it is not necessary to review traffic data. As static IP addresses are assigned to an individual user for a longer period, the ISP can simply view its own records on the users of assigned IP addresses. In the Appellate Court's opinion, this procedure does not interfere with the constitutionally protected secrecy of communication under Article 37 of the Constitution. Hence, the police can obtain information about the holder of a static IP address directly from the ISP, without a court order.[79]

The Appellate Court in Maribor, however, extended the findings from the Benedik case to static IP addresses as well in two of its cases where the suspects had been identified by the police through their IP addresses obtained in a criminal

78 | Zuiderveen Borgesius, 2017, p. 136.

79 | Judgments of the Appellate Court in Ljubljana II Kp 50685/2012, 22. 3. 2018, III Kp 16465/2017, 6. 3. 2019, and V Kp 1896/2017, 12. 12. 2019.

investigation in another country.[80] The Appellate Court noted the ECtHR's emphasis that the subject of assessment was not whether the applicant had a legitimate expectation of privacy regarding the dynamic IP address but whether he had a legitimate expectation of privacy regarding the disclosure of his identity through that IP address. Hence, the ECtHR's judgment in the Benedik case did not legitimize the acquisition of a user's static IP address without a court order. An IP address, regardless of whether it is a static or dynamic IP address, is traffic data that falls within the framework of communication privacy according to Article 37 of the Constitution and not only within the framework of information privacy according to Article 38 of the Constitution. Therefore, a court order was necessary to obtain subscriber information associated with the static IP address from the ISP.

The Supreme Court has not yet decided on the dilemma, but it stated in a recent judgment that if the subscription data of IP addresses are really never made public, then there are no valid reasons for a legal distinction between static and dynamic IP addresses. However, in the concrete case, the Supreme Court was not convinced by the lower courts' finding that the convicted persona used a static IP address. It also pointed out that the findings of the challenged judgment did not reveal any circumstances that would indicate that the convicted person waived their privacy or anonymity when uploading or publishing the image file despite using a static IP address.[81] Based on these hints, it seems likely that the Supreme Court will follow the position of the Appellate Court in Maribor, so that in terms of communication privacy, dynamic and static IP addresses will be given the same level of protection. This seems appropriate because it reflects the actual reasonable expectation of privacy of Internet users rather than relying on a rather technical detail whether the ISP has had a look at traffic data or at subscriber information.

6. Conclusion

We have established that the privacy of IP addresses can be protected both under the rules for the protection of personal data and under the right to communication privacy. Both aspects of privacy are closely related and interconnected, yet the distinction between them remains relevant owing to the different conditions for interference with both rights. In privacy law, the issue is whether the information is private or revealed by the person. In data protection, however, one must ascertain whether the data subject has given valid consent for the processing of their personal data.[82]

Under the criteria developed by the CJEU in Breyer, a dynamic IP address constitutes personal data in the hands of any party that either has or can lawfully obtain sufficient additional data to link an IP address to a specific person's identity.

80 | Judgments of the Appellate Court in Maribor II Kp 50396/2011, 9. 10. 2018, and II Kp 5584/2016, 14. 2. 2020.
81 | Judgment of the Supreme Court of Slovenia I Ips 16465/2017, 28. 1. 2021.
82 | Bygrave and Tosoni, 2020, p. 185.

It remains to be seen whether the same rule will apply to static IP addresses or whether these will always be considered personal data. In the Benedik case, the ECtHR confirmed that an IP address is an integral part of not only information privacy but also communication privacy. The crucial criterion is whether the Internet user has had a reasonable expectation of privacy regarding the disclosure of his identity through the IP address. Again, it remains to be seen whether this reasoning will also be applied to static IP addresses, but the recent case law of Slovenian courts seems to be moving towards uniform treatment of both types of IP addresses.

It seems that the courts have a growing awareness of the privacy implications of IP addresses and the increasing possibilities of abuse in combination with the processing of other metadata that keeps accumulating online and can be used to identify and profile any Internet user. This corresponds to the CJEU's comment in the Tele2 Sverige case that metadata are no less sensitive with regard to the right to privacy than the actual content of the communications.[83]

83 | CJEU judgment in joint cases C-203/15 and C-698/15 Tele2 Sverige v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, 21. 12. 2016, para. 99.

Bibliography

Brkan, M. (2014) 'Varstvo osebnih podatkov v spletnem okolju' in Damjan, M. (ed.) *Pravo v informacijski družbi.* Ljubljana: GV Založba, pp. 67–88.

Brkan, M. (2019) 'The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning', *German Law Journal*, 20(6), pp. 864–883; https://doi.org/10.1017/glj.2019.66.

Bygrave, L.A., Tosoni, L. (2020) 'Article 4(1). Personal data' in Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L. (eds.) *The EU General Data Protection Regulation (GDPR): A Commentary.* 1st edn. Oxford–New York: Oxford University Press, pp. 103–115; https://doi.org/10.1093/oso/9780198826491.003.0007.

Cerar, M. (2009) 'Vrednotna izhodišča varstva informacijske zasebnosti', *Podjetje in delo*, 35(6–7), pp. 1403–1413.

Daly, M. (2022) 'Is there an entitlement to anonymity? A European and international analysis', *European Intellectual Property Review,* 35(4), pp. 198–211.

El Khouri, A. (2017) 'Dynamic IP Addresses Can Be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger's Cat', *European Journal of Risk Regulation,* 8(1), pp. 191–197; https://doi.org/10.1017/err.2016.26.

Golobinek, R. (2021) 'Zadeva Benedik in vprašanje sodne odredbe za podatke o uporabniku naslova IP', *Pravna praksa*, 40(47), supl., pp. II–VI.

Hrustek, N. A., Matijašević, N. (2018) 'Pravica do zasebnosti na svetovnem spletu', *Dignitas*, 55/56, pp. 193–204.

Klemenčič, G. (2011) 'IX. Splošno o komunikacijski zasebnosti' in Šturm, L. (ed.) *Komentar Ustave Republike Slovenije: dopolnitev – A*. Kranj: Fakulteta za državne in evropske študije, pp. 519–565.

Kranenborg, H. (2021) 'Article 8 – Protection of Personal Data' in Peers, S., Hervey, T., Kenner, J., Ward, A. (eds.) *The EU Charter of Fundamental Rights: a commentary.* 2nd edn. Oxford–New York–Dublin: Hart Publishing, pp. 231–290; https://doi.org/10.5771/9783748913245-231.

Križnar, P. (2017) 'IP-naslov za potrebe kazenskega postopka', *Pravna praksa*, 36(14), pp. 16–20.

Križnar, P. (2018) 'Benedik proti Sloveniji', *Pravna praksa*, 37(19), pp. 6–8.

Lesjak, B. (2019) '37. člen (varstvo tajnosti pisem in drugih občil)' in Avbelj, M. (ed.) *Komentar Ustave Republike Slovenije, 1.* De Nova Gorica: Nova univerza, Evropska pravna fakulteta, pp. 356–361.

Lesjak, B. (2022) 'Zakaj je naslov IP osebni podatek po GDPR', *Pravna praksa,* 41(27), pp. 14–15.

Mangan, D. (2021) 'Article 7 (Private Life, Home and Communications) – Respect for Private and Family Life' in Peers, S., Hervey, T., Kenner, J., Ward, A. (eds.) *The EU Charter of Fundamental Rights: a commentary.* 2nd edn. Oxford–New York–Dublin: Hart Publishing, pp. 151–194; https://doi.org/10.5771/9783748913245-151.

Murray, A. (2010) *Information Technology Law: The Law and Society.* 1st edn. Oxford: Oxford University Press.

Pirc Musar, N. (2018) 'Benedik v Slovenia: Dynamic IP and Communication Privafcy', *European Data Protection Law Review*, 4(4), pp. 554–562; https://doi.org/10.21552/edpl/2018/4/22.

Pirc Musar, N. (ed.) (2020) *Komentar Splošne uredbe o varstvu podatkov.* 1st edn. Ljubljana: Uradni list RS.

Schabas, W. (2015) *The European Convention on Human Rights: a commentary.* 1st edn. Oxford: Oxford University Press.

Skubic, Z. (2016) 'Hramba določenih spletnih osebnih podatkov zaradi obrambe pred kibernetskimi napadi', *Pravna praksa*, 35(49–50), p. 47.

Stalla-Bourdillon, S., Knight, A. (2016) 'Anonymous Data v. Personal Data – False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data', *Wisconsin International Law Journal*, 34(2), pp. 284–322.

Zagozda, G. (2022) 'Zakaj naslov IP ne bi smel biti zaščiten podatek po GDPR', *Pravna praksa,* 41(8), pp. 10–11.

Zuiderveen Borgesius, F. J. (2017) 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition', *European Data Protection Law Review*, 3(1), pp. 130–137; https://doi.org/10.21552/edpl/2017/1/21.