Chapter VIII

The Right to Privacy in the Digital Age: A Slovenian Perspective

Matija Damjan

1. Introduction

The right to privacy protects individuals against intrusions into the intimacy of their private life by public authorities, by business entities and by other people. Modern liberal constitutional systems have long recognized privacy as a fundamental right. As such, the right to privacy is an expression of the liberal concept of negative freedom, which must be appropriately supplemented by the concept of positive freedom.[1] Although the need for privacy is generally accepted in the abstract, its precise definition is elusive, as an individual's autonomous private sphere is a multifaceted concept and the social, economic, and technological circumstances that interfere with it are constantly evolving.[2]

In the digital age,[3] privacy is more exposed than ever before, since information and communication technologies, which surround and accompany us everywhere, can easily be (mis)used to invade and closely track individual's private lives, both online and in the real world.[4] Police forces, intelligence agencies as well as private

1 Cerar, 2009, p. 1403; Humble, 2021, p. 6.
2 Rengel, 2014, p. 37; Hartzog, 2021, p. 1677.
3 The digital age, also known as the information age, is a historical period beginning in the late 20th century with the introduction of the personal computer, in which the economy and most aspects of everyday life are shaped by digital information and communication technologies. Bugarič in Damjan, 2014, p. 9.
4 Hrustek and Matijaševič, 2018, p. 193.

Matija Damjan (2023) The Right to Privacy in the Digital Age: A Slovenian Perspective. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 273–309. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_8

sectors have many gadgets available to intrude into individual's privacy, e.g., IMSI catchers, Trojan Horses viruses, CCTV with miniature cameras, drones, etc.[5] The United Nations General Assembly's Resolution on the right to privacy in the digital age[6] noted that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception, and data collection, which may violate or abuse human rights, in particular the right to privacy, and is therefore an issue of increasing concern.[7] The advancement of information technologies also brings a corresponding increase in the risks to privacy. Hence, privacy law must constantly reshape itself to meet the new privacy threats brought about by new technologies.[8]

The purpose of this chapter is to examine how the protection of individuals' privacy in the digital environment has evolved in the legal system of the Republic of Slovenia to consider the use of modern technologies. As a detailed analysis of the multitude of contemporary privacy issues is not feasible within the scope of a chapter, the overview of the general legal framework for the protection of privacy will be followed by a selection of notable cases concerning the right to privacy in the digital environment that have been dealt with by the Slovenian courts and other competent authorities in the recent years. Upon this analysis, we will establish the recent developments in the field and try to assess whether the courts are able to cope with the "digital" privacy issues based on existing rules or whether more specific regulation is necessary *de lege ferenda*. The study of Slovenian case law will allow the reader to compare the findings with the salient issues pointed out in other national chapters, to discover common underlying topics concerning the right to privacy in the digital environments, which might show a need for further European Union (EU) legislative action, particularly concerning cross-border activities and effects.

The chapter will start with an overview of the development of the Slovenian constitutional grounds for the protection of privacy as a fundamental right, operating in the wider context of the European and international human rights law, as well as an outline of the general Slovenian legislation relating to the right to privacy, and the bodies tasked with protecting it in Slovenia. This will be followed by an examination of specific measures for the protection of privacy in various fields of law: civil law, criminal law, and administrative law. After an overview of the available protection measures in the respective area, each of the subchapters will focus on selected issues of privacy in the digital age, that is the cases where these measures come into play

5 Pirc Musar, 2018, p. 559.

6 Resolution adopted by the General Assembly on December 18, 2013, No. 68/167. The right to privacy in the digital age.

7 The resolution was adopted in the wake of the whistle blower Edward Snowden's revelations about mass surveillance programs run by run by national intelligence agencies with the cooperation of telecommunication companies. Joyce, 2015, pp. 271–272; Humble, 2021, p. 1.

8 Rengel, 2014, p. 42.

and that have been discussed in Slovenian case law or at least legal theory. A conclusion will sum up the findings.

2. The evolution of the right to privacy as a fundamental right in Slovenian law

2.1. Constitutional basis for the protection of privacy

The right to privacy has been recognized in Slovenian law for quite some time, even if initially as a rather vague notion. The Constitution of the Socialist Republic of Slovenia[9] of 1974, which applied in Slovenia while it was a constituent part of the former Yugoslavia, did not use the term "right to privacy" but provided constitutional grounds for the protection of privacy in Art. 216, which guaranteed the "inviolability of the integrity of the human personality, of private and family life as well as of other personality rights." This provision was contained in the chapter on freedoms, rights and duties of people and citizens and was interpreted in legal theory as establishing a specific personality right to inviolability of private life.[10]

Nevertheless, the legal protection of privacy started developing in earnest only after the right to privacy was expressly recognized in Slovenia's new constitution adopted in December 1991, which is still in force today. The general right to privacy is guaranteed in Art. 35 of the Constitution of Republic of Slovenia,[11] which protects the inviolability of the physical and mental integrity of every person as well as their privacy and personality rights. This is a wide overarching clause on the right to privacy, setting out a general sphere of individual's privacy, without expressly defining it. The general provision is then supplemented by the more detailed protection of several specific aspects of privacy in the following articles. This nomotechnical approach embraces privacy as a concept with multiple overlapping dimensions.[12]

The first of the specific aspects of the right to privacy is the protection of spatial privacy, defined in Art. 36 of the Constitution, which provides for the inviolability of home. The essence of the right is that no one may, enter the dwelling or other premises of another person without a court order, nor may they search these premises, against the will of the resident. Subject to conditions provided by law, an official may enter the dwelling or other premises of another person without a court order and may in exceptional circumstances conduct a search in the absence of witnesses, where this

9 Official Gazette of the Socialist Republic of Slovenia, No. 6-44/74 et seq.
10 Finžgar, 1985, p. 121.
11 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.
12 Cf. Hartzog, 2021, p. 1679.

is necessary for the direct apprehension of a person who has committed a criminal offence or to protect people or property. The inviolability of the home is based on the territorial conception of privacy, historically conditioned by the protection of private property, the preservation of the autonomy of family life and the physical separation of the public and private spheres of residence.[13]

Art. 37 of the Constitution protects communication privacy, i.e., the privacy of correspondence and other means of communication. According to established constitutional case law, the protection of communication privacy cannot be limited to the content of communication, but the same right also protects data on the manner in which communication took place, who established it, with whom it was established, where it was established from and whether it took place at all.[14] Only a statute (adopted by the National Assembly) may prescribe that based on a court order the protection of privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time where such is necessary for the institution or course of criminal proceedings or for reasons of national security.

Art. 38 of the Constitution guarantees the protection of personal data and prohibits the use of personal data contrary to the purpose for which it was collected. The Constitution mandates that a statute (adopted by the National Assembly) must regulate the collection, processing, designated use, supervision, and protection of the confidentiality of personal data. Everyone has the right of access to the collected personal data that relates to them, and the right to judicial protection in the event of any abuse of such data. In Slovenian constitutional law, data protection is usually understood as an aspect of the general right to privacy rather than a separate right (which is the case in EU law).[15] That is why data protection is also referred to as "information privacy" in the constitutional context.[16] Due to the technical capacity to store monitored and intercepted communications, the protection of information privacy is closely linked to the right to communication privacy. Information obtained through an invasion of communication privacy is, as a rule, personal data that is subject to the protection of Art. 38.[17]

Privacy as a protected constitutional value is also reflected in constitutional provisions on the right to the protection of human personality and dignity in Art. 21 and the freedom of conscience in Art. 41 of the Constitution. However, the fragmentation of the general right to privacy into the listed articles should not mislead—it only serves to prescribe specific conditions for the permissibility of interferences

13 Klemenčič in Šturm, 2011, Art. 37, p. 3.

14 Ibid. p. 4.

15 The right to data protection covers both the 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 EU Charter of Fundamental Rights are closely connected but separate. Kranenborg in Peers et al., 2021, pp. 237–239.

16 Cerar, 2009, p. 1409; Brkan, 2014, p. 70.

17 Klemenčič in Šturm, 2011, Art. 37, p. 3.

with each specific category of privacy. For example, data relating to communication protected by Art. 37 enjoy a higher level of protection than other personal data. Whereas either a clear statutory basis or the affected individual's consent are sufficient to collect personal data, any interference with communication data requires a court order which can be obtained only if necessary for criminal proceedings or the security of the state (and not for any other, albeit legitimate and constitutionally permissible goal).[18] In this regard, the Slovenian Constitution sets a higher procedural threshold for the permissibility of public authorities' invasion int o the communication privacy than international human rights documents and most other constitutions.[19] Communication privacy and information privacy are clearly two aspects of the general right to privacy that are potentially most affected in the digital age, since almost any aspect of one's private life can now be invaded and recorded by electronic means and then transmitted and processed in the form of digital information, usually consisting of personal data. Accordingly, most attention will be paid to these aspects of privacy later in the chapter.

All the cited constitutional provisions protection different aspects of privacy are contained in the chapter of the Constitution dealing with human rights and fundamental freedoms. Thus, the general personal right to privacy in all its emanations is elevated to the level of a human right, which means that it is exercised directly based on the Constitution and can be limited only by the rights of others and in cases where the Constitution allows it (Art. 15 of the Constitution).[20] All individuals enjoy the right to judicial protection of their right to privacy. According to Art. 23 of the Constitution, everyone has the right to have any decision regarding their rights, duties, and any charges brought against them made without undue delay by an independent, impartial court constituted by law. To exercise this right, three forms of judicial protection of the right to privacy come into play: civil and criminal proceedings as well as the constitutional complaint proceedings.[21] Of course, the constitutional right to privacy can also be directly relied upon in administrative proceedings.

The Constitution does not mention information technologies or deal with any specific features of protecting the privacy in digital environments. There have been no proposals to update the constitutional provisions in this respect, although there is otherwise no taboo against amending the Constitution in Slovenian legal and political system.[22] So the task of translating the broad constitutional provisions on the right to privacy into concrete rules applying to specific situations where privacy may be threatened in the new technological context fell to the legislation and the interpretation of fundamental rights in case law.

18 VSRS II Ips 473/2005 and II Ips 474/2005, 10. 10. 2007.
19 Klemenčič in Šturm, 2011, Art. 37, p. 8.
20 Hrustek and Matijaševič, 2018, p. 195.
21 Ibid. p. 201.
22 Eleven amendments to the Constitution have been adopted since its entry into force in 1991, the latest one in 2021.

2.2. Right to privacy in international documents on the protection of human rights

Apart from its own constitutional provisions, Slovenia is also bound to protect the right to privacy by international human rights documents that guarantee this fundamental right. The Universal Declaration of Human Rights states in Art. 12, "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his [or her] honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." Similarly, the International Covenant on Civil and Political Rights provides everyone with legal protection against arbitrary or unlawful interference with their private life, family, home, or correspondence, and provides protection against unlawful insults and reputational damage (Art. 17). The European Convention on Human Rights defines the right to privacy in Art. 8 as "the right to respect for private and family life, home and correspondence."[23] This demonstrates that the right of privacy is universally recognized as a fundamental right which exists as a universal principle of human existence.[24]

These provisions of international treaties have direct effect in Slovenian legal system since Art. 153 of the Constitution provides that all legislation must be in conformity with generally accepted principles of international law and with valid international treaties ratified by the National Assembly. The decisions of the ECtHR are also an important source of law that should be considered when interpreting the provisions of the Slovenian Constitution concerning the corresponding human rights.

The Charter of Fundamental Rights of the European Union also guarantees the right to physical and mental integrity (Art. 3), respect for private and family life (Art. 7) and the protection of personal data (Art. 8). These provisions can be relied upon in Slovenia based on Art. 3a of the Constitution, which allows the transfer of the exercise of a part of Slovenia's sovereign rights to international organizations based on respect for human rights and fundamental freedoms, democracy, and the principles of the rule of law. Since Slovenia's accession to the EU in 2004, this is the constitutional basis for the application of EU law in Slovenia. In line with the principle of primacy of EU law, the Charter's provisions have precedence over any conflicting national laws, which gives them a quasi-constitutional character. Although the Slovenian Constitution sets a higher standard of protection of specific aspects of the right to privacy, particularly the communication privacy, the decisions of the CJEU concerning the Charter's provisions on this right can also be an important source of law.

The provisions of the Constitution and of the mentioned international human rights documents, apart from the EU Charter,[25] have been drafted before the outset

23 See Schabas, 2015, pp. 369–388.

24 Humble, 2021, p. 19.

25 The EU Charter uses the term communications instead of correspondence in Art. 7, precisely to account for technological developments. Mangan in Peers et al., 2021, p. 161.

of the digital age. Nevertheless, with proper interpretation, they can well be applied to protect against intrusions into privacy by digital technologies and for the protection of privacy in the digital environment. Of course, the application of the constitutional rules to specific aspects of privacy in the digital age is detailed in special legislation (as discussed later in this chapter) and further developed in case law, particularly by the Constitutional Court.

2.3. The definition of the right to privacy in the Constitutional Court's case law

The Constitution does not define the content and scope of the right to privacy. As we have mentioned, it is in fact a rather complex concept containing many aspects. As the ECtHR stated in *Bensaid v. the United Kingdom*,[26] "private life" is a broad term not susceptible to exhaustive definition.[27] Therefore, the contours of the right to privacy as a fundamental right in the Slovenian legal system have been drawn by the Constitutional Court's case law dealing with specific situations where this right was infringed upon or came into conflict with other rights. The Constitutional Court defines privacy as an individual's sphere into which no one may interfere with without special legal authority. The right to privacy establishes a circle of intimate personal activity, where individuals can decide for themselves, with the guarantee of the state, which encroachments they will allow. The Court held that Art. 35 of the Constitution, by protecting the inviolability of a person's physical and mental integrity as well as their privacy and personality rights, guarantees the general privacy right that also ensures the general freedom of action.[28] The latter encompasses the principle that in a state governed by the rule of law, everything that is not forbidden is allowed—not the other way around. Hence any prohibition or command is an interference with the constitutionally guaranteed freedom of action.[29] The Court stated that the inviolability of privacy establishes a circle of intimate personal activity, within which individuals may decide for themselves which interferences they will allow.[30]

Privacy constitutes a set of human activities, feelings and relationships characterized by the fact that individuals form and maintain them alone or in an intimate community with their loved ones, and which provide a sense of security before the unsolicited intrusion of the public or of anyone uninvited.[31] Based on these views, the subject of privacy protected by the Constitution is defined functionally and spatially. The functional aspect protects from disclosure individuals' personal affairs, which they wish to keep hidden and which are considered private by their nature or

26 Application no. 44599/98, judgment of 6. 2. 2001, para. 47.
27 As to different theoretical definitions of privacy and the right to privacy, see Rengel, 2014, pp. 39–40 and Humble, 2021, pp. 4–6.
28 U-I-137/93, 2. 6. 1994; U-I-290/96, 11. 6. 1998.
29 U-I-234/97, 27. 11. 1997.
30 Up-50/99, 14. 12. 2000.
31 Up-32/94, 13. 4. 1995.

according to moral and otherwise established rules of conduct in society (e.g., sexual life, health status, confidential conversations between relatives, diary entries).[32] The spatial aspect of privacy protects individuals from disclosure of their conduct in places where they reasonably expect to be left alone. Apart from one's home, individuals' privacy is protected in every place where they can reasonably and clearly for others expect not to be exposed to the public eye.[33]

The right to privacy is not an absolute right but is limited by the protection of the rights and benefits of others and by the individual's behavior in public. As a social being in constant contact with other people, no person can completely avoid the fact that, for various reasons and inclinations, others are also interested in them and their private life. Therefore, the concept of reasonable expectation of privacy is essential in defining the legally protected private sphere.[34] It is composed of two elements: the expectation of privacy and the reasonableness of the expectation. Accordingly, the area of privacy can be divided into three spheres in descending order of intimacy:

- intimate and family life (very private information);
- private life that does not take place in public; and
- public life.[35]

In general, the less intimate the area of an individual's private life, the less legal protection it enjoys when it comes into conflict with the interests and rights of other individuals. In assessing the admissibility of an interference with an individual's right to privacy, the characteristics of the person whose right is being infringed must also be considered. Apart from private individuals, whose private life is most strictly protected, there are two groups of public persons: relative persons of public life who are known to the public only after one, exceptional event, and absolute persons of public life who regularly appear in the media and are of interest to the public. The Constitutional Court held that in reporting the life events of absolute and relative persons of public life, it is permissible to describe without the person's consent, the circumstances pertaining to the character, actions, and thoughts of these persons in relation to their public engagement. Reporting about their intimate life, however, is not permissible without the affected person's consent.[36]

Apart from defining the scope of the right to privacy in general terms, the Constitutional Court has also dealt with several specific aspects of this right in relation to digital technologies. This constitutional case law will be discussed in the context of different legal fields in which the issues arose.

32 U-I-272/98, 8. 5. 2003.
33 U-I-25/95, 27. 11. 1997.
34 Farmany in Avbelj, 2019, Art. 35, p. 12.
35 Up-50/99, 14. 12. 2000.
36 Farmany in Avbelj, 2019, Art. 35, p. 24.

2.4. Right to privacy of legal entities

An important decision of the Constitutional Court recognized that legal entities also enjoy the right to privacy, albeit to a limited extent.[37] The Constitutional Court assessed the constitutionality of a provision of the Prevention of Restriction of Competition Act (ZPOmK-1),[38] which authorized the Competition Protection Agency of Slovenia[39] to initiate an investigation of a company's business premises in connection with proceedings for breaches of competition rules. The agency is an independent administrative authority, responsible for the enforcement of antitrust and merger control rules in Slovenia. The Supreme Court, which referred the issue for review of constitutionality, suspected that entry into business premises, their inspection and review of business documentation, as well as electronic devices and carriers could interfere with the company's right to privacy guaranteed by the Constitution and should therefore only be ordered by a court of law rather than an administrative agency.

The Constitutional Court noted that the Constitution does not expressly grant any fundamental rights to legal persons. However, it is clear from established case law that they must inevitably be able to hold certain constitutionally protected rights, such as the right to property and constitutional procedural guarantees. However, the level of protection of those rights depends on the nature of the right in question and the characteristics of the affected legal entity. The right to privacy of legal entities had not thus far been recognized and the Competition Protection Agency as well as the government of Slovenia contended in the proceedings before the Constitutional Court that legal entities should not enjoy constitutional protection of privacy.

The Constitutional Court underlined that a legal person is an artificial creation of the legal order, derived from the natural persons' right to organize in this way to realize their interests and exercise their rights, such as the right to free economic initiative. For the existence of a legal person and its normal functioning, it is important to have a reasonably protected internal sphere in which the purpose of its establishment can be exercised in peace by its members and personnel. Therefore, the Constitutional Court concluded that the Constitution gives legal persons the ability to protect the information on their business activities against arbitrary interferences by the state or private individuals. The field of privacy of a legal entity has both a spatial aspect (business premises in which it operates) and a communication aspect (possibility of free and uncontrolled distance communication). However, both aspects need to consider the specific nature of a legal person and its operation.

When it comes to the spatial aspect, it is first necessary to separate the business premises of a legal entity, which are intended for the public from those that are not generally accessible to the public. A legal entity only enjoys the right to privacy in

37 U-I-40/12, 11. 4. 2013.
38 Official Gazette of RS, No. 36/08 et seq.
39 The Agency's website at http://www.varstvo-konkurence.si.

business premises that are not generally accessible to the public. The Constitutional Court followed the case law of the ECtHR, which held that certain business premises must be interpreted as the "residence" of a legal person.[40] However, to devise a solution workable under the higher procedural threshold for permissible invasions into the spatial and communication privacy, the Constitutional Court further divided the expected privacy of legal entities into two circles in which the expectations of the legal entity to be left alone differs significantly.[41]

The wider, outer circle of privacy reflects the fact that the Constitution curtails the right of free economic initiative by authorizing the legislature to lay down the conditions and manner of conducting economic activity to protect other constitutional values, such as a healthy living environment. It follows that legal persons cannot expect the state not to supervise their operations to ensure compliance with these regulatory requirements. In this wider, external circle, a legal person enjoys only the general protection of privacy guaranteed by Art. 35 of the Constitution. Interferences with this circle of privacy are admissible if they pursue a constitutionally admissible aim and if they are proportionate. Accordingly, entering business premises and their visual inspection by the competent authorities without opening any hidden compartments and seizing documentation, electronic equipment and any other objects located therein cannot be considered an interference with the legal person's spatial privacy.

The narrower, inner circle of privacy is defined as the internal, covert operation of a legal entity. Interventions in this circle involve the competent bodies' powers to carry out a detailed search of business premises, including their hidden parts, against the legal entity's will, to obtain information, seize documents and other data carriers to investigate the legal person's compliance with the legal rules. Interference with the inner circle of a legal person's privacy is subject to the same conditions as intrusions into the privacy of a natural person's home. This means that it is permitted based only on a court order, as required by Art. 36 of the Constitution.

Legal entities can also expect privacy regarding their distance communication that they consider secret and do not want to disclose. Therefore, legal persons are also entitled to the protection referred to in Art. 37 of the Constitution under which restrictions on the communication privacy of a legal person are permissible upon a court order when necessary for the initiation or course of criminal proceedings or for the security of the state. Here, the Constitutional Court followed the ECtHR's case law which also extended the protection of the privacy of correspondence to legal persons regarding electronic data on a computer system.[42]

Accordingly, the Constitutional Court annulled the provisions of the Competition Protection Act, based on which the Competition Protection Agency held the power

40 See ECtHR cases *Niemietz v. Germany*, 16. 12. 1992, and *Société Colas Est and Others v. France*, 16. 4. 2002.

41 Stoilovski and Lekić, 2013, p. 10.

42 *Wieser and Bicos Beteiligungen GmbH v. Austria,* 16.10.2007.

to authorize on its own the necessary intrusions in the spatial and communication privacy of legal entities when investigating anti-competitive conduct of companies. The Court concluded that the Agency must first obtain a court order expressly authorizing the exercise of its investigating powers in each case involving the search of business premises and the intrusion into the legal entities' inner circle of privacy.

3. General grounds for protecting the right to privacy in Slovenia

3.1. General legislation on privacy

There is no single piece of legislation in Slovenia regulating specifically the protection of the right to privacy, neither as a general *sedes materiae* nor as a special regulation focusing on a specific area in which the issue of privacy arises, such as the digital environment. No such new general legislation concerning the right to privacy is currently planned either. Therefore, the legislative framework does not contain a comprehensive definition of the scope and content of the right to privacy. Nevertheless, the courts generally follow the positions of the legal theory, which usually defines the right to privacy as the limit to which society can intrude on an individual's affairs. The right to privacy is considered both a personality right protected by civil-law instruments, and a human right protected by the Constitution and international human rights instruments.[43] Personality rights belong to every person equally and protect his or her unique personality, i.e., the individual's physical and moral essence. They are personal, non-property rights of private law and they apply *erga omnes*, meaning that anyone—either another individual or the state—is prohibited from interfering with these rights. This reflects the negative aspect of personality rights. However, personality rights also have a positive content in the sense that they allow their holder to directly enjoy a certain personal value, and sometimes even dispose of it.[44] Privacy is one of such personal values.[45]

In line with the Constitution's division of Articles concerning the right to privacy, the legal theory generally divides privacy into the following categories:

- information privacy, which covers the collection and management of private and personal data (also known as personal data protection),
- privacy of the human body, which covers genetic and other investigations of bodily fluids, tissues, or orifices,

43 Hrustek and Matijaševič, 2018, p. 193.

44 Finžgar, 1985, pp. 38–39; Novak, 2000, pp. 991–999.

45 Others being, e.g., physical and mental integrity, physical integrity, honor and reputation, personal name and personal image, etc.

– communication privacy, which guarantees the privacy of mail, telephone conversations and other forms of communication; and
– spatial privacy, which limits intrusion on privacy at work or at home.[46]

Slovenian legislation contains no specific rules protecting the privacy of weaker parties, such as children, seniors, or patients. The protection of children's privacy in school and online has been discussed a lot, lately in particular in connection with distance learning during the COVID-19 lockdown.[47] However, this is based on the general rules on the protection of privacy and personal data, as well as the legislation regulating the educational system. The privacy of patients and their personal data are protected by the Patients' Rights Act (ZPacP),[48] which also regulates electronic waiting lists for doctor's appointments.

The rise of work from home via electronic communications during the recent pandemic has emphasized the need to protect the workers' privacy.[49] The Employment Relationships Act (ZDR-1)[50] generally requires the employer to protect and respect the employees' personality and privacy. However, it does not lay down more concrete rules concerning the use of e-mail, Internet and smartphones, etc. Digital technologies certainly benefit the workers' productivity, yet they also enable the employer to collect the employees' personal data (whom they call, which websites they visit, where they are located, etc.). It would be disproportionate to expect that employees would never use their professional equipment for private purposes, and *vice versa* to never use their own devices for work related purposes.[51] The potential conflict between the employer's and the workers' interests in this regard are not specifically regulated and will have to be resolved based on the general principles of privacy protection in the workspace.

3.2. Legislation on privacy in the digital environment

In the absence of general provisions on privacy, several specific aspects of privacy protection, however, are considered in sectoral regulations. The rules on data protection and on privacy in electronic communications are especially relevant for privacy in the digital environment.

The Personal Data Protection Act (ZVOP-1)[52] defines the rights, obligations, principles, and measures for the processing of personal data in the field of direct marketing, video surveillance, biometrics, etc. The rules of ZVOP-1 have been to

46 Hrustek and Matijaševič, 2018, p. 194.
47 Stopar, 2018, pp. 32–33.
48 Official Gazette of RS, No. 15/08 et seq.
49 Cf. Krapež, 2020, p. 1166.
50 Official Gazette of RS, No. 21/13 et seq.
51 Zupančič, 2015, p. 22; Lengersdorf Medjedovič and Sotlar, 2020, pp. 8–9.
52 Official Gazette of RS, No. 86/04 et seq.

a large extent superseded by the GDPR,[53] which directly applies. Nevertheless, a new legislative act is still required to supplement or interpret the provisions of the GDPR, e.g., by providing a legal basis for imposing fines for breaches of personal data protection rules. However, as of September 2022, the new draft Personal Data Protection Act (ZVOP-2) remains in the governmental procedure and is unlikely to be adopted soon due to the end of the legislative term of the current parliament.

In May 2022, the Information Commissioner warned that Slovenia should urgently adopt appropriate regulations for the implementation of the GDPR and thus resolve the legal uncertainties in ensuring the constitutional right to personal data protection. In the absence of a relevant law, companies, individuals, the public sector, and other organizations face daily ambiguities as to which act regulates specific issues, and the Commissioner cannot impose administrative sanctions under the GDPR due to the lack of procedural rules. Since ZVOP-1 remains in force, the regulation of individual areas, such as video surveillance, biometrics, or the transfer of personal data to third countries, diverges from the GDPR or remains partly unregulated, e.g., protection of privacy in employment relationships, personal data processing for research purposes or for the purposes of freedom of expression and information as well as the control over personal data protection in the judiciary. The absence of legal regulation also does not allow for the effective implementation of measures envisaged by the GDPR to ensure compliance, such as codes of conduct and the possibility of certification.[54]

Rules of the E-Privacy Directive[55] have been transposed in Electronic Communications Act (ZEKom-1),[56] which stipulates that communications and related traffic data may not be stored without the consent of the user, except for the purposes of transmission or traffic management and billing for services. An exception is the storage of communications for the purpose of proving commercial transactions, but users must be informed in advance of the storage, the purpose of the storage and the duration of the storage. The providers of electronic communications are obliged to take all technical and organizational measures to ensure network security. They are obliged to provide users with privacy, which covers the content of communications, traffic data, location data and the facts and circumstances of unsuccessful attempts to establish connections. Traffic data relating to subscribers and users that have been processed and stored by the operator must be deleted or modified in such a way that

53 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.

54 Agencija RS za varstvo konkurence, 2022.

55 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, *OJ L 201, 31.7.2002, pp. 37–47.*

56 Official Gazette of RS, No. 109/12 et seq.

they cannot be linked to a specific or identifiable person once they are no longer needed to transmit messages.[57]

ZEKom-1's provision on the treatment of users' terminal equipment as part of the private sphere is also important as it gives the user's terminal equipment the status of a private space in which an individual can justifiably expect privacy. Regarding web cookies,[58] the law stipulates that the users must be able to reject them, and at the same time must be made aware of what information the web server stores on their terminal equipment using a cookie. The processing of personal data collected by the provider of a publicly available electronic communications service for marketing purposes is not permitted without the user's consent (opt-in approach). Additionally, service providers must always inform users about what data they are processing, for what purpose and how long this information will be stored.

ZEKom-1 initially also contained provisions[59] requiring mandatory retention of traffic data by the ISPs, including users' IP addresses, in line with the Data Retention Directive.[60] However, following the invalidation of the Directive by the CJEU in the case *Digital Rights Ireland*,[61] the Slovenian Constitutional Court annulled these provisions of ZEKom-1 as it held that they disproportionally interfered with the right to the protection of personal data.

A proposal for a new, updated Electronic Communications Act (ZEKom-2), which will transpose the rules of the European Electronic Communications Code (Recast)[62] remains in parliamentary procedure.

3.3. Institutions tasked with protecting the right to privacy

The most important institutions providing effective protection of the right to privacy are the general courts providing judicial relief in both civil and criminal matters, as well as legal remedies against decisions of administrative bodies interfering with the right to privacy. If an individual's privacy was violated by an individual act of state authorities, local community authorities, or bearers of public authority, a constitutional complaint may be lodged before the Constitutional Court against such an act due to the violation of a constitutionally guaranteed human right. However,

57 Hrustek and Matijaševič, 2018, p. 196.

58 Web cookies or html cookies are small blocks of data created by a web server while a user is browsing a website and placed on the user's computer or other device by the user's web browser. Edward and Waelde, 2009, p. 512.

59 Arts. 162–169.

60 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.

61 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.

62 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), OJ L 321, 17.12.2018, pp. 36–214.

a constitutional complaint may be lodged only after all other legal remedies have been exhausted, which means that the affected person must first lodge an appeal or other available legal remedy against the individual act violating their privacy right. Before all extraordinary legal remedies have been exhausted, the Constitutional Court may exceptionally decide on a constitutional complaint if the alleged violation is manifestly obvious and if irreparable consequences for the complainant would result from the implementation of the individual act. If the Constitutional Court finds that a violation has indeed occurred, it may change or repeal the challenged individual act or repeal the executive regulation upon which the challenged individual act was based.

Apart from the courts, two independent bodies have also been important for the development and effective exercise of the privacy right. The Human Rights Ombudsman[63] is specifically mentioned in Art. 159 of the Constitution as an autonomous body tasked with protecting human rights and fundamental freedoms in relation to state authorities, local self-government authorities, and bearers of public authority. The ombudsman is not limited to direct violations of the human rights and freedoms stated in the Constitution but may act in regard of any violation of any individual right by the authorities. He or she can also intervene in the case of unfair and poor management of state officials in relation to individuals. The ombudsman's influence is informal and has no decision-making power, but contributes to the protection and promotion of human rights and fundamental freedoms in Slovenia through the investigation of the complaints, submission of opinions and recommendations to any authority, addressing pressing human rights issues, conducting on-site inspections, conducting human rights education, research, through cooperation with civil society as well as through own initiatives and statements on legislative proposals. The protection of both personal data and other aspects of privacy is among the expressly stated activities of the ombudsman.

The Information Commissioner[64] is an independent state body with competences in the field of two fundamental rights protected by the Constitution—the right of access to public information and the right to the protection of personal data. Since these two rights are closely connected to the right to privacy, the Information Commissioner's opinions have also been important in defining this human right. The Information Commissioner is appointed by the National Assembly of the Republic of Slovenia on the proposal of the president of the Republic of Slovenia for five years and may be reappointed. The body's competences are defined in the Information Commissioner Act (ZInfP)[65] as:

- deciding on an appeal against a decision by which the authority has rejected a request or otherwise infringed the right to access or re-use information of a public nature;
- inspection control over the implementation of regulations on personal data protection;

63 The ombudsman's website at https://www.varuh-rs.si.
64 The Commissioner's website at https://www.ip-rs.si.
65 Official Gazette of RS, No. 113/05 et seq.

– deciding on the appeal when the personal data controller does not comply with the individual's request regarding the right to be informed of the requested data, to printouts, lists, insights, certificates, information, explanations, transcripts, or copies under the provisions of the law governing personal data protection.

The Information Commissioner also acts as the misdemeanor authority responsible for supervising the legislation governing the protection of personal data. Additionally, in accordance with the ZPacP,[66] the Information Commissioner acts as an appellate, inspection, and misdemeanor body. The Information Commissioner's decisions in individual cases as well as the general guidelines and recommendations are influential interpretative sources for data protection rules in Slovenia.

4. Protection measures for the right to privacy in civil law

4.1. Civil-law mechanisms for the protection of privacy

The right to privacy is a human right protected under the Constitution and at the same time a personality right protected by civil-law instruments. The main civil-law mechanism for the protection of privacy is contained in two provisions of the Obligations Code (OZ).[67] Art. 134 of the OZ regulates the request to cease infringement of personality rights, one of which is the right to privacy. Any person can request the court or any other relevant authority to order that action that infringes the inviolability of the human person, personal and family life or any other personality right be ceased (in case of a still lasting infringement), that such action be prevented (if the infringement is imminent) or that the consequences of such action be eliminated (where the infringement has ceased but its consequences remain). The court or other relevant authority may order that the infringer cease such action, with the failure to do so resulting in the mandatory payment of a monetary sum to the person affected, levied in total or per time unit.

In addition, Art. 179 of the OZ allows the court to award to the injured party just monetary compensation for mental distress suffered owing to the infringement of the right to privacy as a personality right—if the circumstances of the case, particularly the level and duration of distress, justify it. This compensation is independent of the reimbursement of material damage and may be awarded even if there was no material damage.

66 Official Gazette of RS, No. 15/08 et seq.
67 Official Gazette of RS, No. 83/01.

4.2. The right to be forgotten in Slovenian civil law

The right to be forgotten as an aspect of the general privacy right was first decided by the Slovenian Supreme Court in 2006. The district court rejected the plaintiff's claim for compensation for non-pecuniary damage allegedly caused by the newspaper's publication of his name in a newspaper article on a double murder, which included a "list of the worst murders in Slovenia." The court ruled that the truthful information of a public nature had been published and that the article did not constitute an interference with the plaintiff's privacy and personal rights. The Court of Appeal dismissed the plaintiff's appeal and upheld the first-instance judgment. The court took the position that due to the criminal act committed, the plaintiff became a so-called relative public person, i.e., a person of interest to the public in connection with a certain event. At the same time, the plaintiff did not fall into the category of persons whose personal name cannot be used in certain situations due to the presumption of innocence, protection of the child or the individual's intimate sphere.

The Supreme Court overturned the lower courts' decision.[68] It disagreed with the view that no infringement of the plaintiff's privacy occurred simply because the newspaper had provided the public with real information, and that the plaintiff should be classified as a relative public person without any time limit. It noted that the court should also consider the time dimensions of relevant events, such as the commission of a criminal offense, the finality of a criminal judgment, the termination of serving a sentence and the time of publication of the disputed article. The Supreme Court took the view that the right to privacy alone could not prevent any publication in matters of public interest. To decide whether the defendant's conduct has an element of inadmissibility, it is therefore essential to determine whether the publication of the plaintiff's name and surname (disclosure of the plaintiff's identity) was in the public interest. However, the general interest of the public cannot be equated with the notion of curiosity but must be assessed as a right to comprehensive information in the context of a published article. The defendant compared the double murder discussed in the article with a list of worst murders in the past, in order of severity. The Supreme Court held, however, that in this connection, the disclosure of the plaintiff's identity was not necessarily in the general interest of the public and may constitute an inadmissible interference with the plaintiff's privacy.

A similar conflict was decided on by the High Court in Ljubljana in 2020.[69] The plaintiff requested that a media remove from its website two articles concerning his candidacy for the position of an ECtHR judge, which also mentioned the fact that he had been convicted in criminal proceedings for violence. Alternatively, the lawsuit offered, the media could also move the articles into an online archive accessible only to registered users. The plaintiff argued that the public no longer had a legitimate interest in being informed of these facts as the candidacy process had ended some

68 II Ips 720/2004, 26. 10. 2006.
69 I Cp 2036/2019, 11. 5. 2020.

time ago and the plaintiff had not been selected for a human rights judge in the proceedings. He also demanded monetary compensation for the infringement of his personality right to privacy.

All the plaintiff's claims were rejected. The High Court emphasized that even if the article was no longer relevant from the perspective of the freedom of expression after the completion of the candidacy for the post of ECtHR judge, it was still relevant and of public interest in terms of historical research of this event and the preservation of the spirit of the time (*Zeitgeist*). As to the plaintiff's alternative claim that the article should be moved to the media's online archive, the High Court ruled that such archiving would in fact be a step towards oblivion and would restrict the media's freedom of expression, which primarily guarantees the public's right to information. The High Court drew attention to the criteria set by the ECtHR in relation to the conflict between the right to be forgotten and the freedom of expression.[70] It also emphasized the importance of the topic discussed in the two articles. In addition to the fact that the candidacy for judge of the ECtHR is a (political) issue *par excellence*, as pointed out by the High Court, decisive reasons for rejecting the plaintiff's claims under the right to be forgotten were that the defendant's reporting was factually correct and without a tendency to defile the plaintiff, and that the plaintiff's presumption of innocence was respected (the article stated that it was a first instance criminal judgment). The High Court also pointed out that in a broader social sense, rehabilitation can also be implemented with the right to be forgotten, but not when it comes to "eternally current" topics, such as the topic of candidates for the highest courts in the EU.

The decision of the High Court in Ljubljana is in line with the CJEU's decision in case Google Spain[71] when it comes to weighing the right to forget and the right to freedom of expression.[72] Like the ECtHR in *Wegrzynowski and Smolczewski v. Poland*, the Slovenian court gave due importance to the right of the public to have unhindered and easy access to older media articles, which do not become irrelevant due to the topicality of their subject.[73]

4.3. The permissibility of evidence obtained by secret recording in civil proceedings

The ubiquity of mobile phones in the digital era allows us to quickly take an audio or video recording of any event, including the possible violations of rules to keep the recording for later evidence. If such a recording was made without the consent of the recorded person, this may violate their right to privacy, so the

70 *Węgrzynowski and Smolczewski v. Poland*, 16.7.2013.

71 Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13.5.2014.

72 Mangan in Peers et al., 2021, pp. 182–184; Rengel, 2014, p. 49.

73 Ovčak Kos and Zakonjšek, 2020, pp. 227–228.

question arises as to the admissibility of the use of such illegally obtained evidence in judicial proceedings. In criminal proceedings, the court is expressly prohibited from basing its decision on evidence obtained in violation of constitutionally determined human rights and fundamental freedoms. Civil procedure, on the other hand, does not contain a general rule on the exclusion of illegally obtained evidence. Nevertheless, a civil court has the power to decide what evidence should be taken to establish the decisive facts.[74]

The Supreme Court of Slovenia first ruled on the issue in 1999, when it held that an audio recording of a telephone conversation with another person made by a participant of that conversation should, in principle, be judged in the same way as written notes of the content of the conversation, regardless of the method of recording (handwriting, typewriter, computer) and regardless of the time of recording (during or after the conversation). In any case, such a recording is mainly a support for the writer's memory—his "memory record,"—which can only serve as additional evidence in support of the credibility of the confession, i.e., the verbalization of the "memory record." The court also considered the business nature of the conversation, due to which it could be expected that a third party would be listening to the conversation or that it could be recorded. The court emphasized that a party may refrain from being questioned as a witness about the content of their conversation with another. Otherwise, the party's right to refuse to testify would be circumvented.[75]

The precedent regarding the admissibility of the use of a secretly made recording of a telephone conversation as evidence in civil proceedings was decided by the Constitutional Court in 2004.[76] The Court held that such recording constituted an infringement of the right to privacy which can only be permissible under certain particularly justified circumstances. The taking of such evidence should be essential for the exercise of another constitutionally protected right. In such a case, the court must respect the principle of proportionality and carefully consider which constitutional right should be given priority.

The Constitutional Court rejected the idea that an audio recording of a telephone conversation could be equated with a written record of the conversation. If the recording is made without the knowledge of the affected person, it encroaches on the person's exclusive right to dispose of their own words or voice as the recording can be replayed. The permissibility of the recording therefore depends on whether, given the circumstances of the case, a person could reasonably expect that a third party will not hear them. The right over one's voice does not depend on the content of the conversation, i.e., whether it is of an intimate nature or contains an exchange of secret information, or whether the interlocutors have specifically agreed that the conversation should remain secret. The possibility to change the topic of

74 Potrč, 2021 at: https://www.iusinfo.si/medijsko-sredisce/dnevne-novice/277948. Cf. Wedam Lukić, 1996, pp. 914–921.

75 II Ips 80/98, 25. 3. 1999.

76 Up-472/02, 7. 10. 2004.

the conversation without the person losing the ease of the conversation is covered by the interlocutor's right to decide for oneself and to prepare for the possible legal consequences of the conversation. This possibility is taken away from the person if they are not allowed to decide for themselves whether to allow the content of the conversation to be heard or recorded by someone else.[77]

Referring to the decision of the Constitutional Court, the High Court in Ljubljana refused to take evidence by listening to an audio recording of the creditor's conversation with other parties while signing a statement that was the subject of dispute in the proceedings.[78] The High Court referred to Art. 35 of the Constitution of the Republic of Slovenia on the right of privacy as ensuring protection against secret recording of conversations without the permission of all persons participating. If the conversation is recorded without the knowledge of the affected person, this infringes on their exclusive right to dispose of their own word or voice. After an assessment of proportionality, the court gave priority to the right to privacy over the right to take evidence.[79]

The admissibility of the use of covert audio recordings from criminal investigation in civil law proceedings was dealt with in a different context by the judgment of the Supreme Court from 2020.[80] A newspapers published a series of articles investigating the privatization of a company, in which it reproduced parts of transcripts of the wiretaps of the plaintiff obtained legally by the police during a criminal investigation. The transcripts were published as proof of the journalists' findings in the article. The plaintiff considered that this had unduly infringed on his privacy and demanded payment of damages. The courts of first and second instance dismissed the plaintiff's claim in its entirety and the Supreme Court confirmed their decisions. It noted that in such cases, the right to privacy must be balanced with the right to freedom of expression, taking into account the following criteria developed in the ECtHR's case law: a) whether the information is a contribution to the discussion of general interest, b) whether it concerns a public figure, c) the person's prior conduct, d) the method of obtaining information and its truthfulness, e) the content, form, and consequences of publication; and f) the severity of the sanctions imposed on the journalists or media.

The Court stressed that the plaintiff was a relative public person who must tolerate certain encroachments on his privacy, and the defendant, as a media company, is a "guardian of the public interest," which means that its right to freedom of expression must be particularly protected. The defendant's journalists did not eavesdrop on the plaintiff themselves but obtained wiretaps (which had been obtained legally) from an anonymous source. Prior to publication, all communications concerning the plaintiff's private and intimate life and all information relating to the criminal

77 Potrč, 2021 at https://www.iusinfo.si/medijsko-sredisce/dnevne-novice/277948.
78 I Ip 152/2013, 23. 1. 2013.
79 Potrč, 2021 at https://www.iusinfo.si/medijsko-sredisce/dnevne-novice/277948.
80 II Ips 23/2019, 23. 1. 2020.

proceedings were excluded from the information obtained. The findings show that journalists approached reporting responsibly and published only those contents that were important from the point of view of the discussion in the public interest. The authenticity or veracity of the published content of the wiretaps was never disputed in the proceedings. In individual articles, journalists even explicitly defined why and in what way the public interest is to get acquainted with the published content. In doing so, they followed the standards of journalistic ethics and did not unduly interfere with the plaintiff's privacy.

5. Protection measures for the right to privacy in criminal law

5.1. Substantive criminal law

In its chapter on criminal offences against human rights and freedoms, the Slovenian Criminal Code (KZ-1)[81] incriminates several types of privacy violations: unlawful body search[82], unlawful eavesdropping and audio recording[83], unlawful visual recording[84], violation of the secrecy of communications[85], unlawful publication of private writings[86], violation of the sanctity of dwellings[87], unlawful disclosure of professional secrets[88] and the abuse of personal data[89]. Most of these criminal offences (apart from Arts. 136 and 141) can also be committed with electronic means. To initiate criminal prosecution of these offences, the state prosecutor must first receive a proposal by the affected person, whereas in some of the less severe offences, the KZ-1 leaves it to the affected persons to initiate criminal investigation with a private action. This reflects the fact that these criminal offences are personal in character and can hardly be either discovered or effectively prosecuted without the victim's active cooperation. After all, privacy is a disposable right—just as a person can allow intrusions into their privacy, they can also waive the prosecution of unlawful infringements of their privacy.

An interesting criminal case concerned criminal sanctions for the violation of privacy online in the form of so-called revenge pornography. A man was convicted of

81 Official Gazette of RS, No. 55/08 et seq.
82 Art. 136 of the Criminal Code.
83 Art. 137 of the Criminal Code.
84 Art. 138 of the Criminal Code.
85 Art. 139 of the Criminal Code.
86 Art. 140 of the Criminal Code.
87 Art. 141 of the Criminal Code.
88 Art. 142 of the Criminal Code.
89 Art. 143 of the Criminal Code.

the criminal offence of unlawful visual recording for having published on Facebook a nude photography of his ex-girlfriend after they had had a quarrel. The photo posted on the "wall" of the convict's profile showed a woman's genitals and a hand with a ring with the convict's comment: "Now sue me and make a fool of yourself ;)." He deleted the photo after one hour. The district court found that the defendant was aware that he was making available to the public the victim's picture in which she would be visible and recognizable to others. His intention was to humiliate her and take revenge on her for the reports she filed against him with the police for refusing to serve him alcohol in a bar where she worked as a server. The High Court rejected the convict's appeal and upheld the judgment of the court of first instance. It stressed that the victim agreed to be photographed only with the intention that these photographs remain between her and the defendant who were in an intimate relationship at the time. The unlawfulness of the defendant's conduct would therefore be ruled out only if he also had the victim's permission to publish the photographs on a social network, which he did not have.

The Supreme Court, however, reversed the decision of the lower courts and acquitted the convict.[90] It emphasized that the Criminal Code protects only a certain aspect of privacy as guaranteed by the Constitution and does not provide criminal protection from any unlawful encroachment on privacy. Under Art. 138 of KZ-1, an act committed by transmitting or presenting photographs to a third person is punishable only if it involves a photography made without the victim's consent and significantly interfered with the victim's privacy. A broader interpretation that would also incriminate transmitting or showing of a photography that has been made with the victim's consent would go beyond the wording of Art. 138 KZ-1 and would violate the principle of legality in criminal law.[91] The court may not interpret a certain criminal norm in a way that implies a substantive extension of the criminal zone since a legal analogy is prohibited in criminal law.

The Supreme Court pointed out that the issue whether to criminalize the publication of photos and video recordings made with the recorded person's permission but in a manner that significantly infringes on their privacy is to be decided by the legislature. It stressed that this issue is even more relevant today, given the modern technology that allows photos and videos to be published on various social networks, and given that such media often publish content that significantly infringes on privacy, whether obtained with or without permission. The Court further explained that the finding that the victim does not have criminal protection does not mean that she has exhausted the legal protection of her right to privacy as guaranteed by the Constitution since the protection of personal rights is also guaranteed by civil law.

Legal commentators have concluded that the Supreme Court's finding was correct and indicates that the scope of incrimination of unlawful visual recording is too narrow. It is unbearable that the scope of the criminal offence does not cover

90 I Ips 76261/2010-40, 27. 9. 2012.

91 Art. 28 of the Constitution of the Republic of Slovenia.

situations where a person consents to certain recordings during a confidential relationship, but this trust is abused after the termination of the relationship and the publication of the visual recording has serious consequences for the victim.[92]

5.2. Criminal procedure

Criminal Procedure Act (ZKP)[93] provides procedural safeguards for the criminal investigation so that the investigative powers of the police and the state prosecutors are not used in a manner that unduly interferes with the privacy rights. The police can obtain data on traffic in the electronic communications network from the operator and intercept electronic communications in actual time. The use of computers, telephones, and other modern communication equipment to commit criminal offences, however, dictates the acquisition of the relevant data after the communication has already taken place. This can only be achieved by subsequent insight into electronic data carriers. Therefore, the ZKP also regulates acquisition of such data from devices. A court order is required for any major interference with the privacy right, particularly the spatial privacy (the search of one's home) and communications privacy (e.g., wiretapping of electronic communications). Exceptionally, in certain cases, an oral request is sufficient, but a written order must be issued later anyway.

The Constitutional Court has on many occasions reviewed the constitutionality of the regulation of special investigative powers of the police, which interferes with the constitutional right to privacy, and has in several cases annulled the regulation of such special measures in the ZKP.[94] Consequently, the provisions of the criminal procedure have been amended fifteen times in the last twenty years.

The Constitutional Court has also dealt with many individual's complaints alleging the violation of the fundamental right to privacy in individual cases. In a recent high-profile case,[95] the Constitutional Court decided on a constitutional complaint against an order by which a district court ordered a search of the premises and additional areas at the address of the National Assembly, used by the complainant who was a deputy of the National Assembly and an alleged accomplice in the criminal offence concerning the abuse of position or trust in a business activity. The complainant alleged that his right to a reasoned judicial decision was violated, *inter alia* because the district court did not substantiate the proportionality between the interference with privacy and the objectives of the ordered search.

The Constitutional Court found that the district court order in fact allowed for an interference with the complainant's right to communication privacy, which applies not only to authorization to seize means of communication that might be found in the complainant's deputy office, but also to the seizure of evidence of communication that

92 Bobnar and Filipčič in Korošec, Filipčič and Zdolšek, 2018, p. 649.
93 Official Gazette of RS, No. 63/94 et seq.
94 Jenull, 2009, pp. 15–17.
95 Up-979/15, 21. 6. 2018.

took place via the communication channels of the National Assembly. Considering the concrete circumstances of the case, employees or holders of public office can reasonably expect, even when using means of communication at work, that persons who are not addressees of such communication will not learn of the content thereof.

According to the Constitutional Court's findings, the district court sufficiently and reasonably justified the probability that evidence of a criminal offence would be discovered in the investigation, and that an investigation was an appropriate measure for achieving the pursued objective. The district court also substantiated the existence of reasonable grounds for suspicion that a serious criminal offence against the economy had been committed. Therefore, a reasonable proportionality between the interference with the complainant's right to privacy, which he as a deputy enjoys in his work environment, and the interests of the criminal procedure was ensured. The Constitutional Court held that the challenged order violated neither the complainant's right to a reasoned judicial decision nor his right to privacy, and thus dismissed the constitutional complaint.

5.3. Communication privacy and metadata

The provision on communication privacy in Art. 37 of the Constitution expressly refers only to "letters" and "correspondence." Yet, the Constitutional Court had no problem interpreting it to protect the privacy of any mode of communication, including any electronic means of communication that did not yet exist in the time when the constitutional provision was drafted.[96] Clearly, the Court does not subscribe to strict originalist or textual interpretation of the Constitution but has searched for the purpose its provisions. The Constitutional Court has also looked at the ECtHR's case law, which adopted the same approach when interpreting the term "correspondence" in Art. 8 of the ECHR.[97] The Constitution protects the privacy of any mode of communication, which should be interpreted in the widest sense of the word.[98] Therefore, apart from old fashioned letters on paper, Art. 37 also protects telephone calls (including VoIP), e-mail, SMS, and instant messaging as well as communication via social networks as long as it is not directed to an indefinite circle of addressees. Regardless of the technology used, the protection extends to any communication that is not public and about which a person can reasonably expect their privacy. The content of communication is immaterial: written, audio and pictorial messages are protected as well as any objects sent. What matters is that the message transmits information to the person involved in the communication.[99]

Under Art. 37 of the Constitution, any interference with communication privacy requires both an express legislative basis as well as a court order. The higher

96 Up-106/05, 2. 10. 2008.
97 Schabas, 2015, p. 400.
98 Up-106/05, 2. 10. 2008.
99 Klemenčič in Šturm, 2011, Art. 37, p. 18–20.

threshold of constitutional protection of communication privacy compared to other spheres of privacy is because remote communication is conducted via post office or via a telecommunication or computer network over which the sender has no direct control. Hence, communication is even more vulnerable to interference by the state or uninvited third parties.[100]

In telephone conversation and any other remote communication carried out by modern telecommunication means, not only the content of the conversation, but also other information related to the communication (metadata) can enjoy constitutional protection. We can distinguish between three sets of data: data on the content of the message (media, communication); data necessary to establish and maintain communication, i.e., traffic data (communication partners, time, duration, etc.); and location data.[101] The protection of the latter two categories can be a more complex legal issue than the (undisputed) legal protection of the content of the communication itself. Traffic and location data are processed to enable the transfer of communications in the electronic communications network (also due to the operation of the network itself) or to enable the billing of the service. Traffic data indicate the origin, destination, route, time, date, scope, duration, or type of service.[102] Location data are defined as any data processed in an electronic communications network or within (public or private) electronic communications services indicating the geographical location of terminal equipment. Traffic data are any data processed for the purpose of transmitting communication over an electronic communications network or for the purpose of charging for it. The trend of processing or storing traffic, location, and related data collected by electronic communications providers is strengthening with the development of technology and the expansion of various services.[103]

A concrete case concerned a criminal investigation of a legally seized mobile phone and SIM card. A complainant who had been convicted of the illicit manufacture and trade in narcotics based on the data obtained from his SIM card (a list of telephone numbers and text messages) 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 holding that the subject of the protection of communication privacy also includes any data on telephone calls that are an integral part of communication. Accordingly, the data obtained from the printout of the telephone memory should be considered as an integral part of communication privacy. Therefore, obtaining information on the last made calls and last missed calls and examination of the content of the SMS message stored on the phone were held to be intrusions into the communication privacy for which a court order is required under. The Court pointed

100 Klemenčič in: Šturm, 2011, Art. 37, p. 19.

101 Lesjak in: Avbelj, 2019, Art. 37, p. 9.

102 "Origin" refers to the telephone number, IP address, or similar identification of the communication unit provided by the service provider; the destination indicates the destination to which the communication at source is intended; the term "type of service" refers to the form of service used in the network (data transmission, e-mail, etc.). Lesjak in: Avbelj, 2019, Art. 37, p. 10.

103 Lesjak in: Avbelj, 2019, Art. 37, p. 10–12.

out that such interference was admissible under Art. 37 of the Constitution only if the following conditions were met: (1) the interference was prescribed by law; (2) the interference was allowed based on a court order; (3) the duration of the interference was precisely determined; and (4) the interference was necessary for the institution or course of criminal proceedings or for reasons of national security.[104]

Regarding online communication, the Constitutional Court's case law defined when an IP-address can be considered private.[105] In the first case,[106] the complainant, who was sentenced for possessing and distributing child pornography, had been identified by the Slovenian police, based on the data obtained by the Swiss police, through the IP address assigned to his computer. The complainant used the P2P file-sharing network Razorback in which any user of the site could view the IP addresses of other users uploading or downloading files. The Slovenian police, without obtaining a court order, requested a Slovenian Internet service provider to disclose data regarding the user to whom the IP address had been assigned. During the house search, the police found one of the seized computers contained files with pornographic material involving minors. The court convicted the defendant and both the Court of Appeals, and the Supreme Court rejected the allegation of illegally obtained evidence.[107]

The Constitutional Court repeated that the subject of protection afforded by Art. 37 of the Constitution is the communication regarding which an individual legitimately expects privacy. Although the IP address must be regarded as traffic data enjoying protection under communication privacy, the complainant waived the expected privacy in the present case, as he did not demonstrate that his IP address was in any way concealed or inaccessible, and the disputed files on his computer could be accessed by anyone who was interested in sharing them. Therefore, the complainant's expectation of privacy was not justified, and a court order was not necessary to obtain an IP address. Since the complainant himself waived the legitimate expectation of privacy, the information on the identity of the IP address user no longer enjoyed protection of privacy in terms of communication privacy under Art. 37, but only in terms of the data privacy under Art. 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.

The convicted person lodged an application before the European Court of Human Rights claiming the violation of his privacy right under Art. 8 of the ECHR.[108] The

104 Up-106/05, 2.10.2008.

105 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. Most dynamic IP addresses can be traced to the ISP to which the user is connected and not to a specific computer. ECtHR case *Benedik v. Slovenia*, 24.4.2018, p. 96.

106 Up-540/11, 13.2.2014.

107 Golobinek, 2021, p. II; Pirc Musar, 2018, p. 554.

108 ECtHR case *Benedik v. Slovenia*, 24.4.2018.

ECtHR followed the assessment of the Slovenian Constitutional Court that the privacy right also refers to obtaining data on the user of a (dynamic) IP address for the purpose of criminal proceedings. Contrary to the Constitutional Court, the ECtHR considered that in the present case the complainant had not waived the expected privacy online by omitting 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 complainant never disclosed his identity in relation to the online activity in question nor was it identifiable by the website provider through an account or contact data. Therefore, the ECtHR concluded that such 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.[109]

The ECtHR also noted that at the relevant time, no regulation specified the conditions for the retention of communication data obtained in criminal investigation and no safeguards against abuse by state officials in the procedure for access to and transfer of such data. The police, having at their disposal information on a particular online activity, could have identified an author by merely asking the Internet service 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. The ECtHR therefore found a violation of Art. of 8 the ECHR, which protects privacy.[110]

The *Benedik* case is important as it confirmed that traffic data, such as dynamic IP addresses, are strongly connected with communication privacy and that national legislatures must comply with the requirements of national constitutions when authorizing law enforcement authorities or other official bodies to limit this fundamental right.[111] In its action report, Slovenia informed the Council of Europe that the Criminal Procedure Code 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 processing of traffic data is required to achieve that.[112] Slovenian courts also gave full effect to the ECtHR's judgment. For example, the Appellate Court of Maribor expressly referred to the ECtHR's findings when holding that a court order was necessary for obtaining of subscriber information associated with the dynamic IP address.[113]

The Constitutional Court also cited the ECtHR's decision in another case[114] where 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

109 Pirc Musar, 2018, pp. 556–557.
110 Golobinek, 2021, p. IV.
111 Pirc Musar, 2018, p. 559.
112 Communication from Slovenia concerning the case of Benedik v. Slovenia (Application No. 62357/14) Revised Action Report (06/10/2021), pts. 15–20.
113 II Kp 50396/2011, 9. 10. 2018.
114 Up-153/17, 9. 9. 2021.

provider of the online forum. The appellant challenged the judgment of the District Court, which found her guilty of the crime 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 Art. 37 of the Constitution, and the acquisition of an IP address in this case constituted an interference with this human right.

5.4. The permissibility of private recordings as evidence in criminal proceedings

The Supreme Court of Slovenia has in several cases ruled on the admissibility of using a private recording made by an individual citizen as evidence in criminal proceedings. In doing so, it weighed between different human rights, namely between the defendant's right to privacy on the one hand and the victim's right to security on the other.[115]

In the first case,[116] the Court held that where the convicted person used a means of communication to threaten the victim, i.e., to commit a criminal offense, he cannot successfully claim that the recording violated his right to privacy. The district court had found the convicted person guilty of endangering security and sentenced him to a suspended sentence. The court found that the convict knew that the victim had filmed him. The convict also admitted in his defense that he said to the victim over the phone that he would strangle him. The Supreme Court held that the right to privacy is not violated if a person allows a third party to record a call or listen to it or if the person agrees to be recorded, thereby expressly or tacitly waiving this aspect of privacy.

A similar decision was made by the Supreme Court in the case where the perpetrator committed a crime over the phone while being recorded and the recording was transmitted to the law enforcement authorities for the purpose of prosecution.[117] The Supreme Court weighed various human rights and, applying the principle of proportionality, ruled that interference with the convict's right to privacy is permissible in a particular case. The audio recording, which the court considered as evidence, was made at the moment of the convict's commission of an extremely serious crime—an

115 Potrč, 2021, at: https://www.iusinfo.si/medijsko-sredisce/dnevne-novice/277948.
116 I Ips 15002/2010, 22. 12. 2011.
117 I Ips 65218/2010, 13. 4. 2017.

incitement to murder. In this specific situation, the right to personal safety or life of the victim undoubtedly took precedence over the convict's personal right to privacy, which was encroached upon by sound recording at the time of the crime and by taking evidence by listening to the recording at the main hearing.

The Supreme Court also weighed between the defendant's right to privacy and the right to personal dignity or to honor and good name of a private prosecutor.[118] It held that an invasion of privacy by secret recording may exceptionally be permissible if especially justified circumstances exist which make the taking of such evidence in criminal proceedings of particular importance for the exercise of another right protected by the Constitution: in this case, this was the right to personal dignity or the right to honor and good name of a private prosecutor.

Frequent cases concern the use of a recording made with pre-installed security cameras. The High Court in Ljubljana, for example, held that video surveillance camera footage of the parking lot in front of the shopping center is not inadmissible evidence even if there was no warning that video surveillance is being carried out.[119] After passing the proportionality test, the court gave priority to the injured party's right to personal security and the right to protection of private property over the defendant's constitutional right to privacy. A different decision would be unreasonable, as it would mean that the defendant's right to privacy when committing a crime outweighs the victim's right to personal safety and protection of private property, and potential defendants could count on greater success in committing crimes.[120]

6. Protection measures for right to privacy in administrative law

6.1. The Information Commissioner's role

The data protection legislation belongs to the field of administrative law, which follows from the manner of prescribing obligations and administrative sanctions for entities of both the public and the private sector in connection with the collection and processing of personal data. The Information Commissioner is the body responsible both for administrative inspection of the compliance with data protection rules and for imposing fines and other administrative sanctions for violations of these rules (see Section 3.3. above). The following are three cases in which the Information Commissioner has recently addressed data privacy issues.

118 I Ips 198/2008, 15. 1. 2009.
119 V Kp 1323/2015, 19. 5. 2015.
120 Potrč, 2021, at: https://www.iusinfo.si/medijsko-sredisce/dnevne-novice/277948.

6.2. Publication of a list of candidates

The National Electoral Commission[121] publishes on its website lists of candidates who participate in the national elections. Apart from the candidates' names, the lists include personal data prescribed by law, including their date and place of birth, address of residence, profession, and the work performed. In 2011, the Information Commissioner initiated *ex officio* inspection proceedings against the National Electoral Commission over the implementation of data protection rules. It decided that lists of candidates who participated in previous elections should be removed.[122]

It instructed the National Electoral Commission to remove from its website lists of candidates voted on in individual constituencies in the elections to the National Assembly in the years 2008, 2004, and 2000. The Information Commissioner noted that the personal data of the candidates in the previous parliamentary elections were published for the purpose of informing the free choice of the voters for which of the candidates to cast their vote. The provisions of the electoral legislation do not imply any other purpose of publishing the candidates' personal data. Therefore, the Information Commissioner concluded that once the election is over, the purpose of processing personal data by publishing it on the website has been achieved, so the lists of candidates must be removed from the website. Even the fact that an individual has participated in election as a candidate is his personal information and the Electoral Commission has no statutory basis for further processing of personal data of candidates in the previous parliamentary elections. The Information Commissioner held that the lists of candidates should be removed from the website from the day when the election results could no longer be challenged by any legal means.

The National Electoral Commission disagreed with the Information Commissioner's decision and challenged it before the Administrative Court. It argued that the purpose of publishing the list of candidates as prescribed by law is to inform voters. The publication of data on who ran for the representative of the people in the past elections cannot cause moral or material harm to any of the candidates. Additionally, if the term of office of an elected member of parliament is terminated early, the next candidate from the list will take his place in the National Assembly. Therefore, candidates, their nominators and voters must know, at least until the end of their term, which candidate is next in line.

The Administrative Court agreed with the arguments presented by the National Electoral Commission, so it reversed and remanded the contested decision of the Information Commissioner.[123] The Court held that the publication of the lists of candidates for elections to the National Assembly was legal until the expiration of the term of office of the current composition of the National Assembly. However, the lists of candidates who ran in the previous elections must be removed from the

121 The Commission's website: https://www.dvk-rs.si.
122 Zagorc and Dolhar, 2011, pp. II–III.
123 I U 2229/2011, 28. 3. 2013.

website, as there is no legal basis for further publication of their personal data on the website.[124]

6.3. Publication of data on recipients of public funds

In 2015, the Commission for the Prevention of Corruption (KPK)[125] published the web application "Supervisor," which made it possible to check the use of public money. Data on natural persons who earned more than EUR 200,000.00 in the period from 2003 to 2015 at the expense of budget users through service contracts were published. Among them was also the plaintiff, who was a professor at the Faculty of Administration at the time of the payments, and the Minister of Higher Education at the time of the publication of the data. The purpose of the KPK was to examine, in the light of the data collected, whether individual cases may have violated the duty to avoid conflicts of interest or the duty to avoid professional activity while performing public office, and to systematically review the justification of service contracts with budget users. Prior to the public announcement of the application, KPK consulted with the Information Commissioner, who believed the publication of personal data on names and amounts related to payments from public money was in accordance with the law.

The plaintiff considered that the publication was illegal and claimed protection against it by suing in an administrative dispute and in civil proceedings. In both cases, the courts of first and second instance rejected her claim, while the Supreme Court decided in her favor.

In the administrative dispute, the Supreme Court emphasized that transparency of the use of public funds is a justified and constitutionally permissible goal, with the requirement to prevent corruption stemming from the general principles of the rule of law. However, those objectives are limited by the protection of human rights and fundamental freedoms, including the protection of personal data. The publication of the plaintiff's personal data could be based on the provisions of the Integrity and Prevention of Corruption Act (ZIntPK)[126] if the KPK completed the inspection procedure on suspicion of corruption in accordance with the said law. However, the KPK did not conduct proceedings against the plaintiff and did not find a violation either before or after the disputed publication of her personal data. The challenged publication of data on payments therefore had no basis in law. ZIntPK provides only a general legal basis for the processing of personal data in connection with the exercise of the

124 Zagorc and Dolhar point out that this distinction may be meaningless given the fact that, in accordance with the electoral legislation, some of the personal data in question must also be published in the Official Gazette of the Republic of Slovenia. The legal regime of publishing in the Official Gazette does not allow the removal of published information after a certain deadline as this would be contrary to the purpose of the existence of a media outlet that also has a historical function. Zagorc and Dolhar, 2011, p. VI.

125 The Commission's website at: https://www.kpk-rs.si.

126 Official Gazette of RS, 45/10 et seq.

KPK's powers; it does not, however, authorize this body to process personal data for the indefinite, general purpose of transparency in the operation of the public sector. For the publication of data in Supervisor to be lawful, the law should have explicitly stipulated what types of personal data the application can contain, the purpose of data use, etc., none of which was the case.[127]

In the civil proceedings, the plaintiff claimed that the state had intervened in her private sphere through its authority and claimed monetary compensation for the infringement. The Supreme Court considered that it was clear from the provisions of the ZIntPK that the KPK did not have the authority to obtain, process, and publish personal data of recipients of public funds in a web application if it did not conduct any proceedings against them. In the concrete case, the KPK acted in a qualified unlawful manner, which was the basis for its liability for damages.[128] In May 2022, the KPK and the plaintiff concluded a court settlement based on which the commission apologized to the plaintiff for illegally publishing her personal data in the Supervisor application.[129]

6.4. Checking digital COVID certificates

At the request of the Information Commissioner, the Constitutional Court assessed the constitutionality and legality of several decrees by which the Government regulated the manner of determining compliance with the condition of recovery, vaccination or testing in connection with the infectious disease COVID-19 (RVT condition).[130] The Information Commissioner asserted that the decrees interfered with the right to protection of personal data without a proper basis for such interference in the law. The contested decrees stipulated that the responsible persons organizing the work process would check the fulfillment of the RVT condition at the entry points, either using the QR code reading application or by inspecting the certificate. Both activities include the processing of personal data, namely health data. The Slovenian government, on the other hand, argued that the Communicable Diseases Act (ZNB)[131] and EU law provided an appropriate legal basis for the processing of personal data. It also referred to the consent of the individual to the processing of his personal data as an appropriate legal basis.

The Constitutional Court held that the determination of the fulfillment of the RVT condition, as follows from the challenged decrees, included the processing of personal data. According to the established constitutional case law, any collection and processing of personal data constitutes an interference with the right to protection of personal data, which is only permissible if the law specifically defines the

127 I Up 310/2015, 24. 5. 2017.
128 II Ips 52/2021, 6.10. 2021.
129 https://www.kpk-rs.si/blog/2022/05/30/opravicilo-komisije-za-preprecevanje-korupcije.
130 U-I-180/21, 14. 4. 2022.
131 Official Gazette of RS, No. 69/95 et seq.

data that may be collected and processed, the purpose for which they may be used, control over their collection, processing and use and protection of secrecy collected personal data.

The Court also rejected the government's view that the GDPR alone could be the appropriate legal basis for the processing of personal data when the processing is required by the state. The GDPR's purpose is to protect the individual from the inadmissible processing of his or her data, and not give a blank check to the state to process personal data. The GDPR allows a Member State to process specific types of personal data, such as health data, for reasons of public interest in the field of public health, such as protection against serious cross-border health risks. However, this can only be done based on provisions of either EU law or a Member State's law, providing for appropriate and specific measures to protect the rights and freedoms of the data subject. The Slovenian Constitution requires that such a basis must exist in a law adopted by the National Assembly rather than in a governmental decree. Regulation 2021/953 on the EU digital COVID certificate[132] also cannot in itself constitute a legal basis for the processing of personal data for the verification of the RVT condition for the purposes determined by a Member State as it still requires the establishment of an appropriate legal basis for such processing in national law.

A person's consent cannot constitute a legal basis for the processing of their personal data if the consent is specified in an implementing regulation or if the law does not specify the conditions under which the consent could be validly given, considering the requirements of the GDPR. A valid consent to the interference with the right to information privacy can only be voluntary. Voluntary consent to the processing of personal data means the absence of external coercion. External coercion does not mean merely physical or mental coercion, but any influence towards giving consent that is not the fruit of an individual's genuine desire. Since individuals' participation in social, political, and religious life would depend on their consent to the processing of personal data to verify the RVT condition prescribed by the state, such consent cannot be considered voluntary.

The Constitutional Court ruled that the two attacked decrees were inconsistent with Art. 38 of the Constitution and annulled them. Yet the repeal will take effect one year after the publication of the Court's decision, thus giving the government sufficient time to amend legislation accordingly while ensuring that there is no legal vacuum in case restrictions need to be reintroduced before such amendments take place.

132 Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic, OJ L 211, 15.6.2021, pp. 1–22.

7. Conclusions

The analysis in this chapter shows that the fundamental right to privacy permeates the Slovenian legal system and cannot be confined to narrower fields, such as personality rights or constitutional law. In the digital era, individuals' private lives are more exposed to intrusions than ever before, particularly through ubiquitous Internet-connected electronic devices, which have made the collection, processing, and transfer of information faster and easier than ever before. Therefore, the significance of the legal protection of privacy in various electronic environments has also increased and more attention is generally paid to possible infringements of privacy. It seems that the pervasiveness of electronic communication technologies has helped individuals recognize that privacy is more than an abstract concept but a value that must be actively protected.[133]

The legal definition of the right to privacy in the digital age cannot remain fixed but must constantly adapt to the development and advances of new technologies that have the potential to interfere with individuals' intimate sphere.[134] Information technologies make it easier to access individuals' personal information online and thus blur the line between public and private information.[135] Therefore, it is suitable that the legislation in force operates with the abstract term "privacy" rather than provide its exact definition, and leaves it to the courts to define the contours of the legally protected sphere privacy in specific contexts.

One of the consequences of the expanded use of electronic communication technologies is that most new types of intrusions into privacy can be interpreted as collection, processing, or transfer of personal data. Hence the focus of today's privacy law has shifted towards issues of data protection as an aspect of information and communication privacy. A possible negative consequence of this trend is that legal approach towards privacy issues all too often consists of formalistic search for express legal basis or individual's consent for data collection and processing. The extent to which people are willing to give away their private data in exchange for digital apps and services might suggest that they do not care about their privacy.[136] However, the number of disputes and other legal proceedings connected with various violations of the right to privacy demonstrate that it remains an important legal value.[137]

The Slovenian Constitution's provisions on privacy have remained unchanged in the last thirty years, yet the perception of the importance of privacy has certainly grown and the measures of protection of the right to privacy have developed in the courts' case law accordingly. The main driver of change in legislation concerning the protection of privacy in the digital context seems to be the EU's regulatory activity,

133 Rengel, 2014, p. 53.
134 Humble, 2021, p. 20.
135 Rengel, 2014, p. 53.
136 Cf. Varanelli, 2019, p. 20.
137 Cf. Cerar, 2009, pp. 1403–1413.

e.g., concerning e-privacy and data protection. If we were to formulate a *de lege ferenda* suggestion concerning the privacy legislation, it is not that additional issues need detailed regulation but the laws implementing EU directives should be more thought out and not just a "copy/paste" of the directives' provisions. Obviously, the new Personal Data Protection Act still needs to be adopted to operationalize the provisions of the GDPR in Slovenian law.

Modern privacy law in Slovenia is to a great extent shaped by the case law of the highest courts, the Supreme Court and the Constitutional Court, rather than through legislation. Both courts rely heavily on the case law of the ECtHR and the EU Court of Justice where available, which causes increasing convergence in dealing with modern privacy issues arise that have arisen in very similar contexts in most European countries. This makes it easier for the courts to cope with the "digital" privacy issues based on existing rules and lessens the need for constant updating of the privacy legislation. Nevertheless, the protection of the right to privacy remains an ever-evolving issue in the digital age and evades any "final" answers.

Bibliography

Agencija RS za varstvo konkurence (2022) *Ob 4. obletnici uporabe Splošne uredbe o varstvu podatkov Slovenija še vedno brez zakona za njeno izvajanje* [Online]. Available at: https://www.ip-rs.si/novice/ob-4-obletnici-uporabe-splo%C5%A1ne-uredbe-o-varstvu-podatkov-slovenija-%C5%A1e-vedno-brez-zakona-za-njeno-izvajanje (Accessed: 26 May 2022).

Avbelj, M. (ed.) (2019) *Komentar ustave Republike Slovenije*. 1st edn. Nova Gorica: Nova univerza, Evropska pravna fakulteta.

Brkan, M., Psychogiopoulou, E. (eds.) (2017) *Courts, privacy and data protection in the digital environment*. 1st edn. Cheltenham: Edward Elgar Publishing; https://doi.org/10.4337/9781784718718.

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 [Online]. Available at: https://doi.org/10.1017/glj.2019.66 (Accessed: 24 October 2022).

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

Damjan, M. (ed.) (2014) *Pravo v informacijski družbi*, 1st edn. Ljubljana: GV Založba.

Edwards, L., Waelde, C. (eds.) (2009) *Law and the Internet*. 3rd edn. Portland: Hart Publishing; https://doi.org/10.5040/9781509955589.

Finžgar, A. (1985) *Osebnostne pravice*. Ljubljana: Slovenska akademija znanosti in umetnosti.

Golobinek, R. (2021) 'Zadeva Benedik in vprašanje sodne odredbe za podatke o uporabniku naslova IP', *Pravna praksa*, 40(47), pp. 2–6.

Jenull, H. (2009) 'Preiskovanje komunikacijske zasebnosti', *Pravna praksa*, 28(10), pp. 15–17.

Hartzog, W. (2021) 'What is Privacy? That's the Wrong Question', *The University of Chicago Law Review,* 88(1), pp. 1677–1688.

Hrustek, N.A., Matijašević, N. (2012) 'Pravica do zasebnosti na svetovnem spletu', *Dignitas*, 55/56, pp. 193–204.

Humble, K.P. (2021) 'International law, surveillance and the protection of privacy', *The International Journal of Human Rights*, 25(1), pp. 1–25 [Online]. Available at: https://doi.org/10.1080/13642987.2020.1763315 (Accessed: 24 October 2022).

Joyce, D. (2015) 'Privacy in the Digital Era: Human Rights Online?', *Melbourne Journal of International Law,* 16(1), pp. 270–285.

Korošec, D., Filipčič, K., Zdolšek, S. (eds.) (2018) *Veliki znanstveni komentar posebnega dela Kazenskega zakonika (KZ-1), 1. knjiga*. 1st edn. Ljubljana: Uradni list RS, Pravna fakulteta Univerze v Ljubljani.

Krapež, K. (2020) 'Posegi v zasebnost (pedagoških) delavcev med epidemijo covid-19 in ponjej – kje so meje dovoljenega', *Podjetje in delo*, 46(6-7), pp. 1166–1177.

Lengersdorf-Medjedovič, T., Sotlar, M. (2020) 'Varstvo zasebnosti pri delu na domu, *Pravna praksa*, 39(37), pp. 8–9.

Novak, B. (2000) 'O naravi osebnostnih pravic', *Podjetje in delo*, 26(6-7), pp. 991–999.

Ovčak Kos, M., Zakonjšek, J. (2020) 'Družbena omrežja, mediji in pravica do izbrisa', *Pravni letopis,* 13(1), pp. 219-240.

Peers, S., Hervey, T., Kenner, J., Ward, A. (eds.) (2021) *The EU Charter of Fundamental Rights: a commentary*. 2nd edn. Oxford: Hart Publishing; https://doi.org/10.5040/9781509933495.

Pirc Musar, N. (2018) 'Benedik v Slovenia: Dynamic IP and Communication Privacy', *European Data Protection Law Review*, 4(4), pp. 554-562 [Online]. Available at: https://doi.org/10.21552/edpl/2018/4/22 (Accessed: 24 October 2022).

Polajnar-Pavčnik, A. (1994) 'Nekateri civilnopravni vidiki varstva pred posegi v človekovo zasebnost', *Podjetje in delo*, 20(5-6), pp. 605–610.

Potrč, J. (2021) *Telefonski ali video posnetek kot dokaz na sodišču* [Online]. Available at: https://www.iusinfo.si/medijsko-sredisce/dnevne-novice/277948 (Accessed: 31 May 2022).

Rengel, A. (2014) 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace' *Groningen Journal of International Law*, 2(2), pp. 33–54 [Online]. Available at: https://doi.org/10.21827/5a86a81e79532 (Accessed: 24 October 2022).

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

Stoilovski, M., Lekić, D. (2013) 'Odreditev preiskave po ZPOmK-1 v nasprotju s pravico pravnih oseb do zasebnosti – kaj pa zdaj?', *Pravna praksa*, 32(22) pp. 10–12.

Stopar, U. (2018) 'Kršitev otrokove zasebnosti na spletu', *Pravna praksa*, 37(16–17), pp. 32–33.

Šturm L., Arhar, F., Plauštajner, K., Rijavec, V., Toplak, L., Blaha, M., Bučar, F., Čebulj, J., Deisinger, M., Dular, J. (eds.) (2011) *Komentar Ustave Republike Slovenije*. 1st edn. Kranj: Fakulteta za državne in evropske študije.

Ude, L. (1996) 'Ustavne podlage za varstvo zasebnosti in osebnih podatkov', *Podjetje in delo*, 22(5–6), pp. 894–902.

Varanelli, L. (2019) 'Pravica do zasebnosti in njeno zanemarjanje', *Pravna praksa*, 38(19), p. 20.

Wedam Lukić, D. (1996) 'Varstvo osebnih podatkov v civilnih sodnih postopkih', *Podjetje in delo* 22(5–6), pp. 914–921.

Zagorc, S., Dolhar, Ž. (2011) 'Pravica biti pozabljen v zvezi z neuspelo kandidaturo na volitvah', *Pravna praksa*, 30(49–50), pp. 2–8.

Zakonjšek, J. (2019) 'Pozor, pravica do pozabe na pohodu! Ali pravica do pozabe ogroža pravico do svobode izražanja?', *Odvetnik*, 21(2), pp. 34–38.

Zupančič, L. (2015), 'Meja dopustnega nadzora uporabe interneta in elektronske pošte na delovnem mestu', *Pravna praksa*, 34(1), pp. 22–27.