# The Right to Privacy in the Digital Age

*Perspectives on Analysis of Certain Central European Countries' Legislation and Practice*

# Studies of the Central European Professors' Network
# ISSN 2786-2518



**Description**
The book series *Studies of the Central European Professors' Network* publishes the results of research by members of the Central European Professors' Network established by the Budapest-based Ferenc Mádl Institute of Comparative Law in 2021. Since 2022, the Network is operated by the Central European Academy of the University of Miskolc, with the cooperation of the Ferenc Mádl Institute of Comparative Law.
The primary aim of the series is to present and address legal issues that are strongly related to the Central European region, taking into account the particular legal traditions, culture, and approach of the countries therein. The authenticity of the books can be seen in the fact that renowned authors from the Central European region write about the legal instruments of countries of the Central European region in English. The book series aims to establish itself as a comparative legal research forum by contributing to the stronger cooperation of the countries concerned and by ensuring the "best practices" and making different legal solutions available and interpretable to all of the states in Central Europe. However, it also aims to provide insights and detailed analyses of these topics to all interested legal scholars and legal practitioners outside the region so that they might become acquainted with the legal systems of Central European countries regarding a great variety of subjects.

# The Right to Privacy in the Digital Age

*Perspectives on Analysis of Certain Central European Countries' Legislation and Practice*

Edited by
**Marcin Wielec**


MISKOLC – BUDAPEST | 2023

STUDIES OF THE CENTRAL EUROPEAN PROFESSORS' NETWORK

**The Right to Privacy in the Digital Age**
*Perspectives on Analysis of Certain Central European Countries' Legislation and Practice*

ISBN 978-615-6474-20-9
ISBN 978-615-6474-21-6 (eBook)

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

Published by

**Central European Academic Publishing**
(Miskolc, Hungary)

The book was published in cooperation with the Budapest-based
Ferenc Mádl Institute of Comparative Law.




The address of Central European Academic Publishing: 1122 Budapest, Városmajor St. 12 (Hungary)

# Contents

# Notes on the Contributors

## Editor and Author

**Marcin Wielec** is a Full Professor and the a Head of the Institute of Justice in Warsaw, Vice-Dean for Student Affairs in the field of "Law", as well as "Man in Cyberspace", and Head of the Department of Criminal Procedure of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw, Head of the research group „The Impact of Digital Platforms and Social Media on Freedom of Expression and Pluralism" in Central European Professors' Network 2021, head of the research group „The Right to Privacy" in Central European Professors' Network 2022 and President of the Polish Association of Comparative Law. A graduate of the MBA program – Top Public Executive at IESE Business School University of Navarra in Barcelona and the Lech Kaczyński National School of Public Administration.

## Authors

**Matija Damjan** is an Assistant Professor for civil and commercial law at University of Ljubljana, Faculty of Law, and secretary general of the Institute for Comparative Law of to the Faculty of Law, where he is also active as a research fellow. In his work, he primarily focuses on the areas of civil law, intellectual property law, and information society law, and has authored more than thirty scientific articles discussing issues in these fields. He is also the author or co-author of several scientific monographs, and co-author of several draft proposals of legislative acts. He is currently engaged in long-term research projects on the legal challenges of the information society.

**Marta Dragičević Prtenjača** is an Associate Professor of Criminal Law at the Faculty of Law, University of Zagreb. She teaches Criminal Law, Juvenile Criminal Law, and Misdemeanour Law at graduate and postgraduate university studies. She is a vice-president of the Croatian Academy of Legal Sciences, a member of the Croatian Association for Criminal Science and Practice, and was a task force member for preparations on International Chamber of Commerce Guidance of Conflict of Interest in Enterprises. She participated in the drafting of several laws and their amendments, including the present-day Criminal Code. She was a researcher on several

projects, including the Zagreb University IPA–2008 project; Croatian Science Foundation project (CSF) Multidisciplinary Research Cluster on Crime in Transition—Trafficking in Human Beings, Corruption and Economic Crime, and the Max Planck (Institute for the Study of Crime, Security and Law) WISKOS project. Currently, she is a researcher in the Central European Professors' Network, and on two CSF project-the Innocence Project in Croatia (CroINOP), and Croatian Misdemeanour Law in the European Context - Challenges and Perspectives (PrePraHR).

**András Koltay** is a Research Professor at the University of Public Service (Budapest). He is also Professor of Law at Pázmány Péter Catholic University Faculty of Law and Political Sciences in Budapest, Hungary. He received his LLM in public law at the University College London in 2006, and his PhD in law at the Pázmány Péter Catholic University in 2008. Between 2018 and 2021, he served as rector of the University of Public Service. He has been the president of the National Media and Infocommunications Authority of Hungary since 2021. His principal research has been concerned with freedom of speech, personality rights, and media regulations, but he also deals with other constitutional questions. He is the author of more than 400 publications, and numerous monographs on freedom of speech; in English: *Freedom of Speech—The Unreachable Mirage* (Wolters Kluwer 2013), *The Troubled Relationship between Religions and the State: Freedom of Expression and Freedom of Religion* (Whitelocke 2017), and *New Media and Freedom of Expression* (Hart 2019). He was a speaker in more than 125 conferences in several countries.

**Bartłomiej Oręziak**, PhD, is the Coordinator of the Center for Strategic Analyzes of the Institute of Justice in Warsaw, a researcher in the Central European Professors' Network 2021 (Research group „The Impact of Digital Platforms and Social Media on Freedom of Expression and Pluralism"). Additionally, he is also a researcher in the Central European Professors' Network 2022 (Research group „The Right to Privacy"), associate at the Faculty of Law and Administration of the Cardinal Stefan Wyszynski University in Warsaw, laureate of the Minister of Science and Higher Education Scholarship for outstanding achievements in science for the academic year 2017/2018. He is the winner of the DOCUP 2020 competition. He is the representative of the Institute of Justice in Warsaw in the Artificial Intelligence Working Group at the Chancellery of the President Council of Ministers, an author of several dozen scientific texts (articles, chapters, glosses, etc.).

**Dušan V. Popović** is a Full Professor of Intellectual Property Law, Competition Law, and Internet Law at the University of Belgrade Faculty of Law. He holds a PhD from the University Paris–Nanterre, an LLM from the University of Nancy, and an LLB from the University of Belgrade. He was visiting researcher at the University Panthéon–Assas (2019), as well as at the Max Planck Institute for Innovation and Competition (2014, 2010), CEIPI—University of Strasbourg (2012, 2011, 2010), and the University of Salzburg (2008). He was a visiting professor at the University of

Lyon III Jean Moulin (2018/2019) and the University of Skopje (2014–2016) and gave a number of guest lectures at different European universities. Dr. Popović served as a Jean Monnet Module Leader on the Erasmus+ project Free Trade Agreements and European Integration of SEE Countries (2017–2020).

**Vanja-Ivan Savić** is a Croatian Professor of Law. He obtained the PhD degree in 2010 at the University of Zagreb. In 2005 he was British Chevening Scholar at The University of Edinburgh. His area of expertise includes Theory of Law and State, Comparative Law, Law and Religion, Corporate Criminal Law and Human Rights. He has held visiting positions at the University of Adelaide, Northwestern and DePaul University and the University of Vienna. Dr. Savić is co-editor (co-edited with Paul Babie) of the book named 'Law, Religion and Love: Seeking Ecumenical Justice for the Other' (Routledge, 2018). He is a member of International and African Consortiums for Law and Religion Studies and Regular member of the Croatian Academy of Legal Sciences.

**David Sehnálek** PhD, is the Vice-Dean for bachelor's degree study and two-year follow-up master's degree programme and an Associate Professor at the Department of International and European Law, Faculty of Law, Masaryk University, where he also completed his PhD studies in the field of private international law. His research focuses primarily on European constitutional law, interpretation of the law, the external relations of the European Union, and European private international law. He is promoting teaching of legal skills through a Czech-Austrian-American project dedicated to this issue which he organizes in close cooperation with the European Academy of Legal Theory and the University of Vienna. He completed an internship at a law firm in Florida (USA) and as a practicing attorney, he focuses mainly on commercial law and private international law. In addition, he publishes scholarly articles in the aforementioned fields of study, and is also an author and co-author of a number of monographs and commentaries.

**Katarína Šmigová**, PhD, is the Dean at the Faculty of Law of the Pan-European University and an Associate Professor at the Institute of International and European Law of this faculty, where she has also completed her doctoral studies in the field of international law. Her scientific research focuses on those areas of international law in which the position of the individual is analyzed, i.e., in particular in the field of international criminal law (LLM in International Criminal Law, Sussex), international human rights law (Diplôme of the International Institute of Human Rights, Strasbourg, as well as lecturer at the European Inter-University Centre for Human Rights and Democratization, Venice) and international humanitarian law (international humanitarian law courses for university teachers, Geneva). In 2016, she also completed a research stay at the Centre for Studies and Research of the Hague Academy of International Law. She is a member of the American Society for International Law and the Slovak Society for International Law at the Slovak Academy of Sciences. She is a member of the International Humanitarian Fact-Finding Commission.

## Reviewers

Balázs BARTÓKI-GÖNCZY
Associate Professor, University of Public Service, Budapest, Hungary

Konrad BURDZIAK
Assistant Professor, University of Szczecin, Poland

Predrag CVETKOVIĆ
Full Professor, University of Niš, Serbia

Lilla GARAYOVÁ
Vice Dean, Pan-European University Bratislava, Slovakia

Anna-Maria GETOŠ KALAC
Professor, University of Zagreb, Croatia

Dubravka HRABAR
Professor, University of Zagreb, Croatia

Jakub MÍŠEK
Assistant Professor, Masaryk University, Brno, Czech Republic

Marcin RAU
Assistant Professor, Cardinal Stefan Wyszynski University in Warsaw, Poland

Rafał WIELKI
Deputy Dean, University of Opole, Poland

---

## Technical Editor

Eszter CZIBRIK
PhD student, Deák Ferenc Doctoral School of Law, University of Miskolc, Hungary

Chapter I

# The Right to Privacy—General Considerations

Marcin Wielec

## 1. Introduction

From an historical perspective, in the life of a community, from time to time, certain circumstances appear that affect their formation, evolution, character, and finally the form of the legal system that organizes the life of these communities. The latter element prompts the emergence of new legal regulations, in line with the well-known Latin dictum, *"Ubi societas, ubi ius"* ("Wherever there is society, there is law"). Often, it takes a moment, or reaching a critical moment in the life of a community, to shape or even discover the new legal parameters. After all, it should be remembered that the atrocities of World War II laid the foundations for the creation of an international judicial body in the form of the International Criminal Tribunal, dedicated to investigating crimes against humanity. It was then that there was a need to administer justice on a global level. Another example here may be the discovery by society and the final formation of basic human rights, which then became a permanent standard of the modern democratic state.[1]

The dynamics of community development is something natural and means that newer solutions require an appropriate organizational and legal framework. We are undergoing the rapid development of new technologies that release new legal challenges., New institutions or tools based on broadly understood new technologies will always need a certain legal framework defining the order of their operation for and

1 Cmiel, 2004, pp. 117–135; Jurczyk, 2009, pp. 29–44; Ishay, 2008, p. 450.

Marcin Wielec (2023) The Right to Privacy—General Considerations. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 11–46. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_1

within the community.[2] It is about mastering them and using only their good sides, although, as we all know, the dark sides of these technologies also exist.

At the center of new regulations is and should always be the human being, with an inalienable dignity. There is no doubt that it is human dignity that is our inherent attribute, a special and recognizable feature, laying the foundation for the further evolution of humanity and related—what is natural—legal systems[3]. Law as a system of norms organizing the life of society must take this dignity into account as the basis of human existence, no matter how modern tools and technologies are created. There is consensus that "no authority: legislative, judiciary or executive, can negate the idea of human dignity as the fundamental principle of law making, applying it or issuing court decisions."[4] Terminologically, "dignity" comes from the Latin *dignus*, which means worthy of respect and worship, or carrying the obligation to be highly respectful.[5] The term connotes pride, honor, ambition, fame, and majesty.[6] There is no doubt at present that dignity is one of the oldest values recognized in society. The essence of human dignity is aptly reflected in the maxim from the Stoics: "the human being is a sacred thing to humankind" (*homo homini res sacra*)[7]—in other words, "dignity is the essence of the human person, that is, it is inseparably connected with every human being, no matter who they are, where and how they live."[8] Hence, no action (public, political, or private) should violate human dignity.[9] Dignity is a value that regulates and determines other areas of human behavior. The universal attributes of dignity are therefore innate, inalienable, permanent, and universal.[10] Therefore, the aforementioned "human rights result from the dignity inherent in man. The authorities do not grant them, but are obliged to obey them. They constitute a category of rights due to man on the public and legal level."[11]

Dignity prompted the emergence and functioning of the broadly understood right to privacy, because synonyms of dignity—pride, honor, ambition, fame, dignity, veneration, respect, etc.—are concepts that also enter the broad orbit meaning of "privacy."

In turn, it is now accepted—and rightly so—that privacy occupies a special position in contemporary catalogues of freedoms and rights and is included in the

2 For example, recently the European Union is working on legal regulations related to the so-called artificial intelligence (see "Proposal for a Regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final).
3 Wermiel, 1998, p. 223; Habermas, 2018, pp. 52–70; McDougal, 1959, pp. 107–136.
4 Sadowski, 2007, p. 25.
5 Jedlecka, 2013, p. 168.
6 Dubisz, 2006, p. 1039.
7 Sadowski, 2007, p. 11.
8 Wojciechowski, 2009, p. 98.
9 Sut, 2000, p. 525.
10 Bucińska, 2001, p. 34.
11 Skorowski, 2003, p. 394.

human rights of the first generation.[12] The latter—that is, human rights of the first generation—are described as "human rights that everyone is entitled to, regardless of their nationality or social position. They are treated as inherent, inalienable rights of the individual, such as the right to life, personal freedom, property, equality, security."[13]

Everyone is equally entitled to natural rights, and no one can be deprived of them.[14] Among these rights is the right to privacy, the root of which is indisputably human dignity. When juxtaposing human dignity with privacy, dignity is an individual's intangible, intimate sphere that gives legitimacy to the right to privacy. Privacy, as broadly understood, falls within the scope of the guarantee of the rights and freedoms of an individual.[15] After all, there is no dispute that these rights are based on the inherent and inviolable dignity of humankind. [16].

Structurally, the term "right to privacy" essentially consists of two different terms and, at first glance, semantically distant concepts, i.e., law/rights, and privacy.

While—obviously—the concept of law is an immanent term associated with communities and their legal systems, defined as a general set of standards of conduct in the form of orders or prohibitions [17], privacy as such is no longer a legal term. It is a term bordering on sociology or psychology etc.

It is assumed that in the legal meaning of the combination of these two concepts, i.e., law and privacy, the common term, i.e., right to privacy, was used by American lawyers S.D. Warren and L.D. Brandeis in 1890 in an article published in the *Harvard Law Review* entitled "The Right to Privacy."[18] This article was a specific response of the authors to what the authors felt was excessive and embarrassing coverage of people's private lives in the press in the form of reports from social meetings organized by the daughter of Sen. Thomas Francis Bayard.[19]

A law "is a set of norms defining the behavior of people, norms established or sanctioned by the state and secured by the state coercion apparatus" (the object approach).[20] A right (also called a specific right) is vested in an entity (subject approach). Hence, privacy can be defined as "a space of free movement, a domain of autonomous activity that is free from the control of other entities, which includes physical space and objects to which others have no access."[21]

12 Banaszewska, 2013, p. 127.
13 Banaszak, 2004, p. 446.
14 Jurczyk, 2009, p. 43.
15 Banaszak, 2004, p. 446; Skrzydło, 2004, p. 166; Witkowski, 2001, p. 102.
16 See justification for the Judgment of the Constitutional Tribunal of April 11, 2000, file ref. Act. K. 15/98, OTK ZU No. 3 (2000), item 86.
17 Kantorowicz, 1958, p. 109.
18 Mielnik, 1996.
19 Motyka, 2010, p. 11.
20 Muras, 2014, p. 5.
21 Pyrciak, 2010, p. 214.

## 2. Research assumptions of the right to privacy

The already proven standards of living in the human community in the form of inalienable values such as dignity or privacy, along with new technologies, has prompted research on the right to privacy as part of the international Central European Professors Network research project, coordinated by the University of Miskolc and the Central European Academy consisting of researchers from Hungary, Serbia, Croatia, Slovakia, the Czech Republic, Slovenia, and Poland. Therefore, it is extremely interesting to study the right to privacy, which must assume a multifaceted, multidimensional, and multithreaded concept, as well as the diversity of legal areas of the indicated countries. Moreover, in the study of the right to privacy, not only legal elements, but also sociological, psychological, and pedagogical elements. intersect.

This book is the result of research by scientists carried out as part of the abovementioned research project. It is an attempt to understand the essence of the right to privacy in the future, considering the current situation, but also trying to predict the effects of the dynamic entry of new trends and instruments in the area of privacy.

In this context, it is valuable to analyze the right to privacy from a comparative perspective, and thus to learn about the perception of the right to privacy from the point of view of several different legal systems. Therefore, the main goal of the research conducted in the framework of the research group is to present in this publication a comparative outline of the right to privacy in Central European countries, especially in modern society.

After all, natural questions arise: How is the right to privacy understood in individual countries? What are the current problems with the implementation of this right? How far-reaching are the interventions of national authorities? Is it possible to define the limits of this interference? What are the cases of interference by international bodies in a given country? What are the national forms of protection of the right to privacy? How is the right to privacy understood by national or international jurisprudence when one of the parties participated in the research? It is also important to indicate the national perspective of understanding, implementing, and protecting the right to privacy. After all, there is no doubt that the right to privacy is one of the most important human rights today.

Subsequent years will create new challenges for human communities and state authorities. Therefore, it is important to anticipate possible controversial situations in the future and analyze the legal situation in each of the countries covered in this project. Therefore, it is of great importance to define the right to privacy in the context of the current legal situation and to try to predict potential solutions related to the right to privacy in the future.

It is also important to indicate the right to privacy as a value, and to define the basis for the protection of the right to privacy, which consists of the essence, content, and scope of the right to privacy.

Another important issue is the means of protecting the right to privacy in civil, criminal, and administrative law, especially considering the specificity of the digital environment. It is also important to recognize the right to privacy from the point of view of judicial decisions depending on a given country.

## 3. Content of the research—General outline

The analyses contained in this book try to answer the above-mentioned research issues closely related to the right to privacy.

The first of the analyses, by Prof. András Koltay, entitled "The Protection of Privacy in the Hungarian Legal System, with Special Regard to the Freedom of Expression" points out from the outset that the current protection of privacy poses a serious challenge to legal systems, especially in light of the proliferation of new technologies for monitoring and registering people. This is a particularly accurate assumption because there is a kind of competitiveness of very important elements of the human community in the form of dynamic development of new technologies and the desire to obtain information by man. Today, information is a very common term, and is one of the most important structural parts of privacy. It is in the name of obtaining information, understanding it, and using and disseminating it that privacy becomes a commodity.[22] There is no doubt that the public is increasingly thirsty for news and information, even confidential info. The balance between the protection of personal privacy and rights, and the public good (freedom of expression, freedom of the press, interest in being informed about public affairs, freedom of information) is difficult to achieve and necessarily remains fragile. In a sense, the importance of the right to privacy increases when the legal norms that ensure—to a greater or lesser extent—the protection of the right to privacy is contained in the provisions of a legal act of the highest order. Of course, today it is the country's constitution. The rank of constitutional regulation for a given legal form makes the protection—in this case of privacy—one of the most important for the legal order of a given country.[23] Hence, we start with an analysis of the right to privacy, starting with the most important legal act in the form of the Basic Law of Hungary.

The Basic Law of Hungary protects the right to the inviolability of private life, and ensures a constitutional level of protection for the home, and for communications and data in the public interest. This is supported by the functioning of a special body for the protection of personal data—the Hungarian Data Protection and Freedom of Information Authority (NAIH).

22 See Barth, 2007, pp. 279–294; Ogbuke, 2022, pp. 123–137; Williams, 2009, pp. 60–67.
23 See Cole and Federico, 2016, pp. 220–237; DeCew and Wagner, 1986, pp. 145–173.

Interesting regulations are also found in civil law in the Hungarian civil code. Protection of civil law is the basic protection for investigating possible breaches of privacy. In Hungarian civil law,[24] they concern protections against the disclosure of confidential information and ensuring the protection of private life. The Hungarian Civil Code has elevated the general protection of private life to the rank of a special personal right, in addition to other established rights also related to privacy, but in a narrower scope (protection of private homes, private information, and personal data, as well as the right to one's name, and the right of protection of one's image and voice recordings).

Another problem identified in Hungarian civil law is the issue of identity disclosure. Identity is also an inherent quality of privacy. Admittedly, it has several threads, because it is also a term on the border of administrative law and civil law, and it can even be combined with criminal law. In the context of privacy, however, this concept is related to the ability to the identification of a person. Hence, identifying a person by revealing their identity is an aspect of privacy, broadly understood.[25] This disclosure may clearly lead to a breach of privacy in various situations related to, for example, court proceedings or "accidental" disclosure of identity. Such a person will become recognizable to the environment in such a way that the published article, photo, etc., do not actually refer to him, and due to the similarity or likeness or identical names, a misunderstanding may arise. Therefore, in this area it is also important to protect the image and voice recordings, which entails the requirement to obtain consent for disclosure. Generally, the subject of protection of the right to one's own image is the image of a person and its consolidation with the use of technology. The production and use of an image of a person or a voice recording requires the consent of the person concerned. On the other hand, the consent of the person concerned is not required for the recording of his or her image or voice if the recording was made in a crowd or in a public appearance. Image protection also concerns the use of the image in public life. In this context, the author notes that sometimes being in a specific public situation is an implicit consent to its exploitation. This is about situations where people participating in public events—even as passive observers—waive their right to privacy to some extent, and even in such cases, photos cannot be published in an offensive or harmful way. There is no doubt, however, that active participants in public events (e.g., speakers) are undoubtedly public figures, while passive observers are not public figures, although photos of such observers may be made public (but not misused), as when the image of police officers during public meetings is published. However, any publication of the image must not be offensive, harmful, degrading, or distorted. The author notes that along with the regulations of substantive law related to the right to privacy, there is also a special court procedure in the matter of image protection. For example, the Hungarian Code

24 See Hamza, 2019, pp. 443–450; Gardos, 2007, pp. 707–722.

25 See Choudhury, 2012, pp. 949–957; Feng et al., 2019, pp. 45–58; Oomen and Leenes, 2008, pp. 121–138.

of Civil Procedure allows for a special mode of claiming the right to protect one's images and voice recordings, the main aim of which is to remove the consequences of the violation as quickly as possible.

An interesting issue is also the requirement of openness of proceedings where the right to privacy is an important element. Open court hearings are a norm. The standard of a democratic state ruled by law requires that the course of court proceedings be transparent. The openness of court proceedings consists in the possibility of becoming acquainted with the course of the court proceedings, unless there are some reasonable limitations in favor of not being fully open to the public. The Basic Law of Hungary requires an open court procedure (public administration of justice). However, the requirement of openness, as an aspect of the right to a fair trial enabling the free transmission of information about court proceedings, cannot be treated as an unlimited right. In informing the public, the media must respect other laws as well. Such rights that may limit publication are the personal rights of trial participants (in particular, the right to protect their image and voice recordings, the right to privacy, and the protection of minors).

Turning to criminal law, in the Hungarian legal system, the author notes that by default, these are individual crimes such as intrusions, breaches of private information, breaches of secret correspondence, the illegal obtaining of data, breaches of trade secrets, the abuse of personal data, and the misuse of data of public interest). On the other hand, the norms of criminal procedure correlated with criminal law focus on the requirement to respect human dignity, because privacy and the right to privacy are fundamentally related to human dignity.[26]

On the other hand, research in administrative law shows that one of the sensitive issues is the protection of personal data. The subject of personal data itself is an extremely important matter, and of a global nature.[27] Personal data is also an important element of privacy.[28] To protect fundamental democratic values, it has become necessary for the state to create restrictions—primarily for itself—to ensure the protection of the personal data of its citizens, and thus their undisturbed privacy. The aim is to provide citizens with "transparency" against others—state and market actors—only to the extent necessary. In administrative proceedings, the law allows for restrictions on the right of access to documents due to the protection of private information and personal data, while the conflict between the right to a fair procedure guaranteed by the constitutional law and the protection of privacy must be resolved by law enforcement authorities on a case-by-case basis.

In the next analysis, entitled *The right to privacy in the European context—insight into the basic issues*, Prof. Vanja-Ivan Savić, analyzes the right to privacy in the legal

26 See Whitehead and Wheeler, 2008, pp. 381–385; Floridi, 2016, pp. 307–312; Moreham, 2008, pp. 231–247.

27 See Tikkinen-Piri, Rohunen and Markkula, 2018, pp. 134–153; Purtova, 2018, pp. 40–81; Custers and Uršič, 2016, pp. 4–15.

28 See Chaudhuri, 2016, pp. 64–75; Bert-Jaap and Leenes, 2014, pp. 159–171; Bygrave, 2001, pp. 277–283.

system of the European continent and selected issues related to privacy, which were the subject of research on the part of national and international judicature. The research approach is interesting here, because the right to privacy is examined from the point of view of axiology. It is axiology as the science of values that sets a very precise point of reference by analyzing the right to privacy as one of the laws shaping the human environment. If we assume that values are absolute, which sets the direction of regulation for the legislature, which will result directly from the needs of society and which will be worth achieving in the legal system, the right to privacy is one of the most important values.[29]

Another point of the analysis is the right to privacy in the context of infection with the COVID-19 virus, as it turns out that epidemiological regulations significantly affect privacy.

The author notes that privacy laws are in fact related to individual privacy rights or expectations regarding privacy and the right to a private and undisturbed life. These features are the very essence of privacy, and therefore the general right to leave everyone in peace. It is the essence of privacy and its legal regulations are among the most important challenges facing us today.[30]

Quoting scientific positions, the author rightly points out that the right to privacy was and still is a "human right" before it became a "well-established fundamental right." The author rightly deduces the right to privacy from the concept of human dignity, clearly pointing out that human rights are a product or derivative of human dignity. In other words, human dignity is the source of human rights and as such occupies a very special position. Therefore, according to the author's view, an understanding of the concept of dignity is necessary to be able to balance the right to privacy and the right to surveillance, as well as the right to privacy and legal state control, which must be: a) justified, b) proportionate, and c) protecting public order. The appeal to dignity in the context of examining the right to privacy is the starting point for any consideration of human rights.[31]

The author also analyzes the right to privacy from the point of view of European law. He states that there is no doubt that privacy matters to the European Union. In this sense, the most visible example of this is the tendency to establish control over the use of data by corporate bodies. These principles show that privacy controls have their limits, which are set out in the relevant legislation—analyzed in this study—and offer guidance in balancing public security with personal and family privacy. Moreover, all this should be analyzed through the lens of public order and public morality.

Another field of the author's analysis is the protection of privacy in family life, with particular emphasis on the protection of children. In general, the protection of children is an exceptionally delicate and important topic, often discussed in legal and

29 See Rössler, 2005, p. 268.

30 See Lilien, 2007, pp. 85–117; Spiekermann, 2012, pp. 38–40; Jensen, 2013, pp. 235–238.

31 See Vaibhav, 2022, pp. 99–116; Ondreasova, 2018, pp. 24–70; Francis and Leslie, 2018, pp. 207–218.

other publications.[32] The author categorically and rightly points out that the family is and should be the cornerstone of European societies and deserves special protection. The author notices and analyzes many international documents that protect family life and are either part of the European legal structure or international pacts and treaties that overlap with European law. In view of the contemporary challenges related to privacy, the author states that the most endangered element in our society is its foundation—the family. There is no doubt that, *inter alia*, the Charter of Fundamental Rights of the European Union contains many provisions regarding the protection of human dignity and guarantees the legal, economic, and social protection of the family, and defines the right to private and family life, home, and personal communication. The right to protect privacy in family life is also embedded in the domestic law of individual ECHR Member States.

There are numerous debates about the extent of state interference in the private life of the family, especially in relation to the parents' right to raise their children in accordance with their philosophical and religious beliefs. There are various aspects of the right to privacy that interfere with family life: a) the parents' right to educate and raise their children, b) the family's right to be protected from outside influences, c) the parents' obligation to take best care of their children's needs and interests, d) the duty of the state to ensure an appropriate and decent legal and then social framework for family life, e) the duty of the state to oversee the educational system for the benefit of children, and f) the duty of the state to interfere in the life of the family in cases of violence, crime, and especially when children require special protection.

The author concludes that the basis of privacy should be sought in the socio-psychological concept, which was gradually introduced into the legal systems worldwide and in Europe. One has to agree with the author that the shape of the right to privacy is not yet definitively defined and the processes of introducing the concept of privacy into the legal systems of European countries are underway to date, and at the same time attempts are being made to find the right balance between individual concepts building the right to protect privacy, on the one hand, and the concepts of security and protection of society as a whole, that is, public morality and public order on the other one.

In the next study, entitled "The Right to Privacy in the Digital Age: A Slovenian Perspective," Prof. Matija Damjan presents how the privacy of individuals in the digital environment is protected in the legal system of the Republic of Slovenia, which naturally functions in the wider context of the European and international human rights framework.

In the Slovenian legal order, the protection of privacy is defined—as in other countries of central Europe—first in the provisions of constitutional rank. Also here, in this study, the provisions of constitutional rank are first presented. It is confirmed

32 Plattner, 1984, pp. 140–152; Van Bueren, 1994, pp. 809–826; Melton and Flood, 1994, pp. 1–28; Rodham, 1973, pp. 487–514.

once again that guaranteeing the protection of privacy in the provisions of constitutional rank is a standard in the constitutional regulations of democratic states. The constitution is the beginning of ensuring the protection of the right to privacy.

The provisions of the Slovenian constitution first provide for the inviolability of the apartment. The issue of the inviolability of the apartment is a complex and important topic. The essence of this law is that no one may enter the dwelling or other room belonging to another person or search this room against the will of the person living in it without a court order. Subject to the conditions provided for by law, an officer may enter another person's flat or other premises without a court order and may, in exceptional circumstances, carry out a search in the absence of witnesses, if this is necessary for the immediate appreciation of the person who committed the crime or for the protection of persons or property. The inviolability of the home is based on the territorial concept 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 the place of residence.

Another component of the right to privacy protected by the provisions of the Constitution of Slovenia is the protection of the privacy of communication, i.e., the privacy of correspondence and other means of communication, including any electronic means of communication that did not exist at the time when the constitutional provision was drafted. "Communication" is understood here as a very broad conceptual component of the right to privacy, which is often emphasized in the literature on the subject.[33]

Another element of the protection of the right to privacy in the Slovenian Constitution is the privacy of information, i.e., guaranteeing the protection of personal data and prohibiting their use contrary to the purpose for which they were collected. After all, personal data is an emanation of privacy. There is a strong link between personal data and the right to privacy.[34]

The author notes that all the cited constitutional provisions protecting various aspects of privacy can be found in the chapter of the Constitution devoted to human rights and fundamental freedoms. The author states that, based on constitutional provisions, the right to privacy in all its manifestations has been elevated to the rank of a human right, which means that it is exercised directly based on the Constitution and may be limited only by the rights of other persons and in cases the Constitution specifically allows. There is therefore no doubt that the right to privacy is one of the human rights.[35]

There is a close link between the right to privacy and judicial protection, as every person enjoys the right to judicial protection when their right to privacy is violated. Everyone has the right to have any decision concerning his rights, duties, and any charges against him taken without undue delay by an independent, impartial

33 Burgoon, 1982, pp. 206–249; Kushelvitz, 1992, pp. 273–284; Trepte, 2021, pp. 549–570.
34 Sobczyk, 2009, pp. 299–318.
35 Diggelmann and Cleis, 2014, pp. 441–458; Roessler, 2017, pp. 187–206.

tribunal established by law. To implement this right, there are three forms of judicial protection of the right to privacy: civil, criminal, and constitutional complaint proceedings, which the author thoroughly analyzes in terms of the examined right to privacy.

Additionally, the study attempts to find a definition of the right to privacy in the jurisprudence of the Constitutional Court of Slovenia. Based on the jurisprudence, the right to privacy is treated as a fundamental right. For example, the author cites several views of the Constitutional Court of Slovenia, which defines privacy as, inter alia, the sphere of an individual's life in which no one can interfere without special legal authorization. The right to privacy establishes a circle of intimate personal activity in which individuals can decide for themselves, with the guarantee of the state, what interference they will allow. By protecting the inviolability of a person's physical and mental integrity, as well as their right to privacy and personality, it guarantees the general right to privacy, which also ensures general freedom of action. The latter includes the principle that in the rule of law, everything that is not forbidden is allowed—not the other way around. Therefore, each prohibition or order constitutes an interference with the constitutionally guaranteed freedom of action. The inviolability of privacy determines the circle of intimate personal activity within which individuals can decide for themselves what interference they will allow. Hence, privacy is a set of human actions, feelings and relationships characterized by the fact that individuals create and maintain them either alone or in intimate communion with their loved ones, and which provide a sense of security against unwanted intrusion by public opinion or anyone uninvited.

The author states that based on these views, the subject of privacy protected by the Constitution is defined functionally and spatially. The functional aspect prevents disclosure of an individual's personal affairs, which he or she wishes to keep secret and which are considered private by their nature or in accordance with moral and other rules of conduct established in society (e.g., sex life, health, confidential conversations between relatives, diary entries). The spatial aspect of privacy protects individuals from disclosing their behavior in places where they reasonably expect to be left alone. Outside the home, the privacy of an individual is protected wherever he or she can reasonably and clearly expect others not to be exposed to the public.

The right to privacy of legal persons is another fascinating discussion. He cites a ruling by the Slovenian Constitutional Court which found that legal persons also had the right to privacy, albeit to a limited extent.

Apart from the indicated regulations of the Constitution of Slovenia, the author states that there is no legal act that would specifically regulate 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 like a digital environment. There are also no plans for new general legislation on the right to privacy at present. Therefore, the legal framework does not provide an exhaustive definition of the scope and content of the right to privacy.

The author's research has shown that the right to privacy is considered both a personal right protected by civil law instruments and a human right protected by the Constitution and international human rights instruments. Personal rights are equally applicable to every human being and protect their unique personality, i.e., the physical and moral essence of an individual. These are personal, non-property private rights and are *erga omnes* binding, which means that no one—neither another person nor the state—can interfere with these rights. This reflects the negative aspect of personal rights. However, personal rights also have a positive content, as they allow their holder to use a certain personal value directly, and sometimes even to dispose of it. Privacy is one such personal value.

The study also includes an analysis of the institutions responsible for protecting the right to privacy. In the Slovenian legal system, the most important institutions ensuring effective protection of the right to privacy are common courts, which provide legal remedies in both civil and criminal cases, as well as remedies against decisions of administrative authorities interfering with the right to privacy. If the privacy of an individual has been violated by individual actions of state bodies, local community bodies or public authorities, a constitutional complaint may be lodged with the Constitutional Tribunal against such action due to the violation of a constitutionally guaranteed human right. The study specifies the basic model of the procedure for lodging a constitutional complaint. If the Constitutional Tribunal finds that a violation has taken place, it may amend or revoke the challenged individual act or revoke the implementing regulation on which the challenged individual act was based. However, this analysis shows that specific measures to protect the right to privacy in civil law are based on the main civil law mechanism for the protection of privacy, contained in two provisions of the Slovenian Code of Obligations, which regulates the demand to cease infringement of personal rights—one of which is the right to privacy. Any person may apply to a court or other competent authority to order the cessation of an activity that violates the integrity of a human person, personal and family life, or any other personal interest (if the violation continues), to prevent such activity (when the violation is imminent), or to remove the effects of such action (when the breach has ceased, but its effects remain). The court or other competent authority may order the infringer to cease such action, and in the event of failure to act, a compulsory payment of a sum of money to the injured person, collected in full or for each time unit.

An interesting point is to pay attention in the study to the so-called the right to be forgotten in Slovenian civil law, first settled by the Slovenian Supreme Court in 2006 as an aspect of the general right to privacy.

Another interesting issue is the admissibility of evidence obtained by secret recording in civil proceedings.

In the area of criminal law under Slovenian law, the right to privacy, on the other hand, is protected by a series of criminal offenses. And so, in the Criminal Code of Slovenia, in the chapter on crimes against human rights and freedoms, the Slovenian Penal Code criminalizes several types of violations of privacy, such as:

unlawful body searches, unlawful wiretapping and audio recording, unlawful visual recording, violation of the confidentiality of communication, unlawful publication of private letters, violation of the sanctity of housing, unlawful disclosure of professional secrets and misuse of personal data. Most of these crimes can also be committed by electronic means. To initiate criminal proceedings for these offenses, the national prosecutor must first receive a request from the injured person, while for some less serious offenses, victims are left with the option of initiating a private criminal prosecution. It should be emphasized that these crimes are personal and difficult to detect or prosecute without the active cooperation of the victim. After all, privacy is an optional right—just as individuals can allow interference with their privacy, they can also refrain from prosecuting unlawful violations of their privacy.

On the other hand, the Criminal Procedure Act provides for procedural safeguards in criminal proceedings so that the investigative powers of the police and prosecutors are not used in a way that excessively interferes with the right to privacy. This area was dealt with, *inter alia*, by the Constitutional Court in Slovenia, which has repeatedly examined the constitutionality of regulations on special investigative powers of the police, which interfere with the constitutional right to privacy, and in several cases has annulled regulations on such special measures in criminal proceedings. The effect of this was that the rules of criminal procedure have been changed fifteen times in the last twenty years. In criminal proceedings, there is also the issue of the admissibility of using private recordings as evidence in criminal proceedings. The measures to protect the right to privacy in administrative law focus mainly on the provisions on the protection of personal data. The author presents case studies in which the information commissioner recently dealt with data protection issues.

The author concludes that the right to privacy is a true fundamental right that permeates the Slovenian legal system and cannot be limited to narrower areas such as privacy law or constitutional law.

The analysis of the right to privacy by Prof. David Sehnálek entitled "The Right to Privacy in the Digital Age in the Czech Republic" shows how privacy is protected in the Czech Republic, but strictly according to the standards of national law not yet covered by unification tendencies at the level of EU law relating to the right to privacy. The main environment for analyzing the right to privacy has become modern digital technologies, and more precisely the impact of their functioning on the protection of privacy. There is no doubt that modern technologies are currently the factor determining new challenges in terms of the scope and type of legal regulations.[36] They influence our social life, influencing them directly, shaping our attitudes and opening up new opportunities.

The analysis is complemented by the presentation of the jurisprudence of the Czech Constitutional Court and its Supreme Court.

36 See general Bielecki et al., 2021; Filiczkowska et al., 2021; Górska et al., 2021; Blicharz et al., 2021; Wielec and Oręziak, 2021a, pp. 113–139; Wielec and Oręziak, 2021b, pp. 121–149; Wielec and Oręziak, 2021c, pp. 117–141; Wielec and Oręziak, 2021d, pp. 101–129.

At the beginning, the author reviews the regulation of the right to privacy at the constitutional level. He points out that the current Czech constitutional legislation on the protection of privacy was adopted in connection with the partition of the former Czechoslovakia. It is contained in several articles of the Charter of Fundamental Rights and Freedoms of the Czech Republic (hereinafter referred to as the "Czech Charter"). These national regulations are complemented by harmonized international and EU regulations on this issue, which, however, are rather present in the Czech judicial practice. Nevertheless, the author notes that the regulation of privacy protection in the Czech Charter is fragmentary and therefore quite complicated. According to this document, the general protection of the right to privacy is ensured by Art. 7 (1) of the Charter, which guarantees the integrity of the person and his privacy. It may be limited only in cases provided for by the law. The essence of the right to privacy protection is defined in Art. 10(1) of the Czech Charter, according to which:

> 1. Everybody is entitled to protection of his or her human dignity, personal integrity, good reputation, and his or her name. 2. Everybody is entitled to protection against unauthorized interference in his or her personal and family life. 3. Everybody is entitled to protection against unauthorized collection, disclosure, or other misuse of his or her personal data.

Partial protection of privacy is ensured by Art. 12 of the Charter, which states that human habitation is inviolable. Art. 13 of the Charter states that, nobody may violate the secrecy of letters and other papers and records, whether privately kept or sent by post or in another manner, except in cases and in a manner specified by law. Similar protection is extended to messages communicated by telephone, telegraph, or other such facilities. In a broader sense, provisions ensuring the protection of privacy can also be included in Art. 15 of the Charter, which guarantees freedom of thought, conscience, and religion. According to the author, there is also a second possible approach to the systematics of regulating the right to privacy in the Constitution of the Czech Republic. In line with this approach, Art. 7 (1) of the Czech Charter refers only to the physical and mental integrity of the person. Therefore, it is not a general clause, but a specific and subject-limited provision. The right to privacy is primarily protected in Art. 10 of the Czech Charter. Therefore, these two provisions overlap when processing personal data obtained because of an interference with the physical and mental integrity, e.g., genetic information, blood chemistry results, etc., as not only Art. 7 but also Art. 10 deals with this issue in its third section.

The author indicates that such an approach is supported by the jurisprudence of the Constitutional Tribunal and seems to prevail, even if it does not correspond to the legislature's original intention. However, it is favored by the system of the Czech Charter, which ranks fundamental rights according to their importance.

The next area of research concerns legal regulations regarding the right to privacy at the sub-constitutional level, e.g., in civil laws protecting the privacy of natural and legal persons.

At the same time, the protection of privacy does not raise any major concerns, but the topic, which includes the possibility of interfering with their privacy or of creating a privacy protection system for a legal person, is extremely interesting. The literature asks whether the privacy of a legal person is possible at all, or whether it is a fiction.

In administrative law in the Czech Republic, the right to privacy primarily concerns the processing of personal data.

On the other hand, the criminal law protects the rights to personality, privacy. and confidentiality of correspondence. In particular, the following crimes are regulated: illegal disposal of personal data, violation of the rights of other people, violation of the confidentiality of correspondence, violation of the confidentiality of records and other private documents, and defamation. The criminal law also protects against cyberstalking.

In the context of privacy and modern technologies, the Civil Code plays a significant role in the civil law of the Czech Republic. This legal act treats privacy protection as follows: (1) The right to privacy protects the dignity and freedom of man and his natural right to care for his own happiness and the happiness of his family or those close to him in such a way as not to cause unjustified harm to others. (2) Private law is based in particular on the principles according to which: a) everyone has the right to the protection of life and health as well as freedom, honor, dignity and privacy.

Interestingly, under Czech law, the right to privacy is not statute-barred, although there are some exceptions that the author mentions and analyzes in depth.

In addition, the protection of privacy in the context of modern technologies in the civil procedural law of the Czech Republic takes the form of a series of procedural rules that are formulated very generally and do not regulate, for example, the heated issue of electronic evidence, which is inherently related to modern technologies. An interesting element of this analysis is the use of digital evidence, which by its nature is an element directly or indirectly related to modern technologies and the fight against cybercrime.[37]

Analyzing the right to privacy in relation to modern technologies in the public law of the Czech Republic, the author notes that special rules apply to work in public administration, including administrative law regarding the possibility of recording the course of proceedings. No one may be forced to do something that is not prescribed by law. There is no provision preventing a party to an administrative procedure from making audio recordings of the hearing, and it does not matter whether it is a public or private proceeding. Therefore, there are no grounds for stating that by making an audio or visual recording of the proceedings, the party grossly disturbs the order and may be asked to leave the hearing. This could only take place in a situation in which making a recording of the administrative procedure would be a gross disturbance of the peace. However, in court proceedings, the possibility of making

37 See Kigerl, 2009, pp. 566–589; Shapiro, 1999, pp. 14–27; Stolz, 1983, pp. 157–180; Hancock, 2000, pp. 306–307; Wible, 2003, pp. 1577–1623; Coleman, 2003, pp. 131–136; Simon, 1998, pp. 1015–1048; Walden, 2004, pp. 321–336; Reidenberg, 2005, pp. 1951–1974.

recordings is clearly regulated, *inter alia*, in the Law on Courts and Judges, which explicitly states that visual or sound transmissions and visual recordings may be made during a court hearing only with the prior consent of the president of the chamber or one judge. Sound recordings may be made with the knowledge of the president of the chamber or a single judge; the president of the chamber or a single judge may prohibit such recordings if the manner of their making may have a negative impact on the course or the seriousness of the proceedings.

The right to privacy also means image protection, which is especially important when recording with a participation of the third party.

The right to privacy in the Czech legal system is also an area of interconnection between civil law and criminal law. Attention is paid to privacy in the light of the Civil Code and to sound, visual, or other recordings made as part of the defense against crime. The analysis is extremely interesting here, because crime victims may defend themselves against recordings that violate the right to privacy, but even this defense has its limits. Such recordings may not be used in an "offensive" manner. Returning, however, to civil and family regulations, the author presents a new phenomenon of violating children's privacy by their parents: "sharenting." This is defined as parents' thoughtless and excessive sharing on the Internet, especially in social media, of an image of their child—photos and videos in which the child can be recognized, without the child's knowledge and consent. The development of information society services, in particular the various social networks, has facilitated the dissemination of information that falls within the scope of privacy. Sharing information about yourself is usually not a problem: part of our freedom is also the freedom to decide which parts of our private life becomes public. However, the situation is more serious when privacy information is published by persons who have a right to do so, but relates to another person who cannot decide for themselves. This usually applies to parents and children, and may also apply to persons deprived of legal capacity and their guardians. In a broader sense, this also includes the activities of schools and kindergartens, which might make what is happening in their institution publicly available in the form of photos or videos, generally through "sharenting."[38]

Another element of the analysis is the intersection between privacy, digital technologies, and Czech labor law. According to the author, it is understandable that employers are interested in using modern technologies to monitor the workplace—and consequently, the employee. The analysis presents the protection of the employer's property interests and the protection of the employee against unjustified interference with their privacy.

Finally, the author's arguments also address the issues of privacy and COVID-19, where several anti-epidemic measures in the Czech Republic based on the use of digital technologies are presented. The Tečka and čTečka applications were introduced, which process the personal data of natural persons. These applications were

38 See Błasiak, 2018, pp. 125–134; Fox and Grubbs-Hoy, 2019, pp. 414–432; Garmendia, Martínez and Garitaonandia, 2022, pp. 145–160; Brosch, 2018, pp. 75–85; Goggin and Ellis, 2020, pp. 218–228.

used to prove and check whether a person had a valid negative test, or had been vaccinated for COVID-19.

In the next analysis, entitled "Privacy and Data Protection in Serbian Law: Challenges in the Digital Environment" Prof. Dušan V. Popović points out that the concept of privacy in Serbian law is a relatively new and modern concept. The meaning of this concept has grown with the development of digital technologies. The introduction of privacy regulations into the Serbian legal order was caused by the international obligations of the Republic of Serbia in the field of privacy and protection of personal data, which in turn result from its membership in the United Nations and the Council of Europe, as well as from its candidate status in the EU. The approach of the Serbian legislature is similar to that of the European Union, as the constitutional right to data protection is regulated separately from the right to privacy in the strict sense. Additionally, for decades, the right to privacy has been protected under national civil and criminal law.

The author presents that in the Republic of Serbia, as in other jurisdictions, there is no unanimously adopted definition of privacy, both in the legal doctrine and in legal instruments. National constitutions, including Serbia's, usually protect the privacy of individuals by referring to: (1) the inviolability of the home; (2) confidentiality of letters and other means of communication; and (3) the protection of personal data. In a broader sense, the right to privacy can also include freedom of thought, conscience, and religion, in the sense that citizens are under no obligation to declare their religious or other beliefs. One must agree with the author that the ubiquity of the Internet, social networks, search engines, and computing clouds, has reduced the right to privacy to the right to personal data protection. Therefore, the protection of privacy in a digital context means, in essence, the protection of data relating to an identifiable natural person. The concept of personal data includes not only names, addresses, and identification numbers, but also any data that can be associated with an individual, such as photos, profiles on social networks, and web browsing history.

In the first part of the analysis, the author examined several international obligations of the Republic of Serbia in the field of privacy and personal data protection, resulting mainly from the legal instruments of the United Nations, the European Convention on Human Rights, and the Stabilization and Association Agreement concluded between the EU and Serbia. The Republic of Serbia's international obligations in the field of privacy and personal data protection derive from its membership of the United Nations and the Council of Europe, as well as from its EU candidate status. The right to privacy enjoys constitutional protection in the Serbian legal system in at least two respects: it protects the inviolability of home, and it protects the confidentiality of letters and other means of communication. Moreover, the Serbian Constitution guarantees the right to the protection of personal data. However, the right to the protection of personal data and the right to privacy should not be treated the same way. The scopes of both rights overlap to a large extent, but there are also areas in which their subjective and objective scopes diverge. In addition, in line with the trends in comparative law, the Serbian legislature, by issuing numerous laws

and executive acts, intervened in the field of personal data protection, primarily in relation to the "traditional" protection of privacy.

The connotations of the protection of the right to privacy in Serbia law are also protected in civil law. Under Art. 157 of the Act on Contracts and Torts, everyone has the right to demand that the court or other competent authority order the cessation of activities that have resulted in violation of the inviolability of a natural person or of family life, and other rights relating to the person. In the event of a breach of privacy, the general principles of civil liability for unlawful acts apply.

The right to privacy is also protected in criminal law. The Criminal Code of the Republic of Serbia provides for several crimes that are directly or indirectly related to the violation of privacy: (1) violation of the privacy of letters and other mailings (including e-mails); (2) violation of the peaceable home; (3) unlawful search of dwelling or person; (4) unauthorized disclosure of a secret; (5) unauthorized eavesdropping and recording; (6) unauthorized photographing; (7) unauthorized publication and presentation of someone else's texts, photos, or recordings; (8) unauthorized collection of personal data; (9) disseminating information about personal and family life; (10) showing, acquiring, or possessing pornographic material, including pornography of minors; (11) using computer networks or other technical means of communication to commit crimes against the sexual freedom of a minor; (12) unauthorized use of or access to a computer, computer network, or electronic data processing; or (13) breach of the confidentiality of official proceedings. In addition to criminal liability, several laws provide for penalties for minor offenses.

The legal framework for the protection of privacy and personal data in the Serbian Republic also includes administrative redress. Pursuant to the applicable regulations, the data subject (the natural person whose personal data is processed) has the right to lodge a complaint with the public information and personal data officer if he or she believes that the processing of his personal data was unlawful. Even though the Republic of Serbia is not yet an EU Member State, the General Data Protection Regulation of the European Union may, under certain circumstances, apply in the Serbian context. This means that companies that have links with the European market must comply with the same data protection standards that European companies apply.

The author's analysis situates privacy as a value that functions in Serbian literature. He emphasizes that in Serbian law, the concept of privacy was initially used to describe the protection of personal and family life, protection of the home, and the protection of correspondence. Today, the concept of privacy is understood rather as the protection of personally identifiable data. The Serbian legal doctrine distinguishes between general personal law and special personal rights. The right to privacy is traditionally classified as special personal rights, along with the right to one's identity, to one's good name (derived from the right to human dignity), and to respect for the deceased.

On the relationship between privacy and data, i.e., the protection of personal data in administrative law, the author shows that the main legal act currently regulating the protection of personal data in the Serbian Republic is the Personal Data Protection Act, adopted in November 2018 and in force since August 2019. This act

defines personal data as any information relating to a natural person whose identity can be determined or identified, directly or indirectly, in particular by reference to an identifier, such as a name and surname and identification number, location data, Internet identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

In conclusion, the author points out that privacy has been directly or indirectly protected in Serbian civil and criminal law for decades. However, the new challenges are precisely the widespread use of the Internet and modern technologies. It was these two factors that raised the issue of privacy and personal data protection, and led to the creation of special protection mechanisms in law. Further developing digital technologies will require additional legislative efforts, especially in the field of mass surveillance and child protection.

The analysis "The Right to Privacy in the Digital Age (from the Viewpoint of the Slovak Legal Order)" was presented by Prof. Katarína Šmigová.

First, Šmigová analyzes the concept of privacy and its contents, as well as the challenges related to this concept in the context of the digital world. The analysis begins with the examination of the provisions of the Constitution of the Slovak Republic and the jurisprudence of the Constitutional Court of the Slovak Republic. The author notes that both the right to privacy and privacy are not defined in the Slovak Constitution. Nevertheless, the Constitution of the Slovak Republic provides guarantees for the right of every individual to integrity and privacy. Limitations on this right can only be introduced in cases expressly provided for in the act. However, the Constitutional Court of the Slovak Republic clarified that the constitutional protection of the right to privacy is related to the inviolability of the person, and therefore privacy is related to the integrity of the body and material values of a private nature. Slovakia's constitutional jurisprudence generally indicates that the protection of private life from being made public must be understood more broadly than the protection of life: it also includes the right to establish and develop relationships with other people, especially in the emotional sphere, to develop and realize one's own personality. The interesting thing about this argument is that originally the right to privacy in the legal order of Slovakia only applied to natural persons. The court has expressly excluded a legal person as a privacy protection entity within the meaning of Art. 16 of the Constitution. Nevertheless, considering the judgments of the ECHR, the jurisprudence of the Constitutional Tribunal changed its interpretation and granted legal persons protection under Art. 16 of the Constitution, therefore legal persons deserve protection not only under the Civil Code, but also under the Constitution.

A more detailed provision relating in a way to the right to privacy can be found in Art. 19 of the Slovak Constitution. According to this article, everyone has the right to human dignity, personal honor, and the protection of one's reputation and good name. In addition, everyone has the right to be protected against the unauthorized collection, publication, or other misuse of personal data. Finally, everyone has the right to be protected against unlawful interference with private and family life. According to the author, the current understanding of the right to privacy was influenced

by the era of lack of freedom in the past. Based on the achievements of constitutional jurisprudence, there was no real public society at that time, so there was no public space, and the protection of privacy was essentially reduced to neighborly or communal conflicts. That is why the specification of the right to privacy was made more specific in the Slovak Civil Code, because it constitutes the basis for the private law protection of personal rights that are part of the right to privacy. The Civil Code deals with the protection of human personality, in particular life and health, civil honor and human dignity, privacy, name, and statements of a personal nature. In addition, the Civil Code regulates the right to protect personal documents, portraits, images, as well as video and audio recordings of a natural person or their statements of a personal nature, which may be produced or used only with the consent of that person, unless they are produced or used e.g., for purposes. official, scientific, or artistic.

The personal goods mentioned in the study are also a special component of the right to privacy. The author of the analysis found that the means of judicial protection of personal rights are, first, a negative action, i.e., a demand that the court rule on the abandonment of unjustified interference, and, second, a restitution action, i.e., satisfactory, i.e., demand that the court rule on adequate redress. These judicial remedies may be used individually or in combination. Their joint application depends on the purpose, e.g., if the unjustified interference with personal rights continues and the right to compensation has arisen, it is possible to bring a negative claim with a satisfactory claim.

The author —like the authors in previous analyses—also sees the problem of the right to privacy in the context of children, especially as they may be victims. Children as victims are a very delicate and complicated problem. Overall, Slovakia is party to all international treaties that deal with the protection of children in the online world.

Moreover, it should be noted that the Slovak legal order also addressed the issue of cyberbullying. The concept of cyberbullying is also a new term introduced on the canvas of dynamically developing new technologies.[39] For several years now, the penal code has allowed the *de facto* prosecution of cyberbullying through the *de jure* prosecution of several other, already-defined crimes. Cyberbullying was *de facto* prosecuted via laws on cyberstalking, blackmail, coercion, sexual abuse, defamation, violation of the rights of others, child pornography (production, distribution, possession), compromising morals, endangering the moral education of youth, and even crimes of supporting and promoting terrorist groups, of producing, disseminating, or storing extremist materials, of denial or approval of the Holocaust, as well as crimes of political regimes, of the defamation of other nations, races, and beliefs, of inciting national, racial and ethnic hatred or threats. Another issue related to the right to privacy is when a person is monitored.

The author also presents the problem of privacy in the context of the systemic transformation in Slovakia. during the Communist regime the State Security Service (Štátna bezpečnosť, or StB) kept files with lists of associates. It was noticed that these collaborators were divided into several groups depending on their level of cooperation, e.g.,

39 Slonje, Smith and Frisén, 2013, pp. 26–32; Olweus and Limber, 2018, pp. 139–143; Sabella, Patchin and Hinduja, 2013, pp. 2703–2711; Langos, 2012, pp. 285–289; Smith, 2008, pp. 376–385.

agents, candidates for cooperation, or informants. After the collapse of the Communist regime, the files of the StB were released (although some of them were destroyed) and several people realized that they were on these lists, refusing to cooperate.

The author also presents specific conclusions about the right to privacy in the digital world. He notes that whether it is digital cameras, satellites, or just what we click on, we must have more explicit rules—not only for governments, but also for private companies. Finally, it is true that the information was difficult to find. Today, however, it is difficult to make a choice. It is important to be aware of and respect the rules that also apply to private individuals, because we never know to whom we are opening the door to our privacy.

Prof. Marta Dragičević Prtenjača, in her chapter entitled "The Report on Privacy and Criminal Law in Croatia—Criminal Offenses Against Privacy in the Croatian Legal System" indicates that although technology is something extremely positive, it also has a dark side. Therefore, privacy and the right to privacy must be protected at the international and national level (constitutional and legislative), as it is a kind of shield against the intrusion of other people and the state, and thus protects individuals and their rights. Its violation must be prohibited, and there must be sanctions for violating it.

The author distinguishes between privacy, the right to privacy, and private space. These are three different terms and should not be understood as synonyms.

*Privacy* is a term that each state defines in its own way (even each legal area has its own definitions). *The right to privacy* is the right of the individual to enjoy privacy, which is protected by various international documents and national constitutions and laws. *Private space* is a space "no one has the right to enter" and in which the individual has the right to enjoy his privacy.

In the Republic of Croatia, the right to privacy is guaranteed by its constitution and the provisions of ratified conventions, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the legislation of the European Union, including implementation of the General Data Protection Regulation. Privacy is also protected by various national laws, such as the Labor Act, the Media Act, the Electronic Media Act, the Consumer Protection Act, and the Electronic Communications Act. The protection of the right to privacy is complemented by the provisions of the Penal Code, which, however, are applied according to the "ultima ratio" principle. Nevertheless, despite so many pieces of legislation directly or indirectly relating to the right to privacy, in Croatia, there is no unique definition of privacy or the right to privacy. In the first place, the right to privacy is guaranteed by the Constitution of the Republic of Croatia in various contexts. Among other things, the protection of various rights and freedoms is regulated by Art. 14 of the Constitution, which states that everyone in the Republic of Croatia, regardless of social origin, sex, race, religion, and other characteristics, has rights and freedoms, and everyone is equal before the law. Rights and freedoms are not absolute. The Constitution in Art. 16 provides the possibility of certain limitations of the guaranteed rights and freedoms: only a statute may limit the rights and freedoms of citizens to protect the freedoms and rights of others, the rule of law, public morality, and health; and any restriction of these rights and freedoms

must be proportionate to the nature of the need to limit the rights and freedoms. The right to privacy, as already mentioned, takes several forms, and various constitutional provisions guarantee its protection, including Art. 34 which guarantees the inviolability of the house as a form of privacy. The provision of Art. 35 guarantees everyone the right to personal and family life, dignity, honor, and good name, while Art. 36 prescribes the freedom and secrecy of correspondence and all other forms of communication. The provision of Art. 37 guarantees the security and confidentiality of personal data, and Art. 40 the right to religion and religious beliefs. All the above articles of the constitution guarantee various forms of privacy and indicate the necessity of their legal protection. Interpretation of the above provisions of the Convention and the Constitution of the Republic of Croatia leads to the interpretation that no one (the government or other persons) may take any action that would restrict the rights of other persons to a greater extent than it results from the relevant provisions of these documents.

One of the most important issues in Croatian law relating to the right to privacy is the provisions relating to the General Data Protection Regulation (GDPR), which is directly applicable and is defined in the Act on the Implementation of the General Data Protection Regulation. Elsewhere in the Croatian legal system, the Media Act defines privacy as family and personal life and the right to live of one's own choice.

The provisions of the Croatian criminal law complement the aforementioned regulations. Criminal law criminalizes a number of crimes against privacy in a special chapter of the Penal Code entitled "Offenses Against Privacy"—including violation of a dwelling or business premises[40]; violation of the secrecy of letters and other parcels[41]; unauthorized sound recording of eavesdropping[42]; unauthorized taking of photos[43]; taking sexually explicit videos without consent[44]; unauthorized disclosure of professional secrecy[45]; and Unlawful Use of Personal Data[46]. Some crimes against privacy can be found in other chapters, as crimes against marriage, family, and children (violation of the privacy of a child[47]), but also in the chapter regulating crimes against the judiciary (identity disclosure of threatened person or protected witness[48]). Important information is that in 2011, Croatia received a new criminal code with a new chapter, "Offenses against Privacy." The subject of protection here is privacy, which, as stated, is not unanimously defined, but it can be said that it is the private sphere of individuals, encompassing the physical and mental interests of individuals, including sex, gender expression, and sexual orientation, as well as personal data, reputation, and photographs.

40 Art. 141 of the Penal Code.
41 Art. 142 of the Penal Code.
42 Art. 143 of the Penal Code.
43 Art. 144 of the Penal Code.
44 Art. 144a of the Penal Code.
45 Art. 145 of the Penal Code.
46 Art. 146 of the Criminal Code.
47 Art. 178 of the Penal Code.
48 Art. 308 of the Penal Code.

The author explicitly believes that the right to privacy is inextricably linked with data, the collection of which, without the knowledge of individuals, is spying. This word is the correct word to describe what is actually happening. Many people do not think about these aspects—maybe they do not want it, or maybe they are not aware of the dangers of a daily visit to the Internet or performing legal actions (e.g., entering into a contract when providing their personal data). But whether we like it or not, the danger is there, and we give our personal data about habits, wishes, and everyday interests to all kinds of people (physical or legal) and entities. Banks, news sites, science networks and journals, almost everyone. Everyone often uses this information for different purposes, unilaterally choosing to store, sort, or even sell it to the highest bidder.

The presentation and analysis of statistical data in this study is very valuable, because the author wanted to directly check how many such crimes were committed between 2016 and 2020. According to data collected both by the Croatian Bureau of Statistics (CBS) and based on research carried out at the Municipal Criminal Court in Zagreb, the most common criminal offense is the Unlawful Use of Personal Data[49], which is represented in over 50% of convictions for criminal offenses against privacy (according to CBS data) and 83% in a survey by the Zagreb Municipal Criminal Court. In the second place is the infringement of the inviolability of a dwelling and business premises[50] of about 30% (according to CBS data), but not so much when the Zagreb Municipal Court survey is questioned (only 0.8% less than 1%). According to CBS data, convictions for unauthorized taking of photos[51] account for approximately 5% of convictions. Interestingly, there is no data available during the observation of the Disclosure of the Identity of a Dangerous Person or a Protected Witness[52]. The crime of the abuse of sexually explicit material[53], also known as "revenge porn," is still a "young" crime (as of July 2021), so it is understandable that we do not have criminal convictions data.

The final analysis is the study by Bartłomiej Oręziak entitled "The Right to Privacy in the Digital Age: A Perspective from the Republic of Poland."

This study deals with the analysis of the right to privacy in the digital age from the perspective of the Polish normative system—that is, the Polish approach to the right to privacy. First, Oręziak discusses the digital reality as a new space for the right to privacy, and attempts to define the right to privacy. The right to privacy is then presented in light of constitutional regulations, then in civil and criminal law, and finally in administrative law. The author notes that Polish law lacks a statutory definition of the right to privacy and the right to privacy itself, but proposes to define the right to privacy as a right of every human being by virtue of simply being human (an element of natural law), to ensure that intrusion into their privacy (e.g., private, family, home, home, communication correspondence), is not legally unjustified

49 Art. 146 of the Penal Code.
50 Art. 141 of the Penal Code.
51 Art. 144 of the Penal Code.
52 Art. 308 of the Penal Code.
53 Art. 144a of the Penal Code.

(horizontal aspect) or unjustified by the proportionality test (vertical aspect), and that there was no interference (protective function) by another private entity or state (positive and negative actions). In the case of an unjustified violation of privacy, it ensures that any damage caused is repaired or restored. This will lead to recognition that the right to privacy is one of the values.[54]

The analysis carried out in this area showed that the Polish Constitution contains several provisions relating to the right to privacy, according to Art. 47 of Polish Constitution, everyone has the right to legal protection of private and family life, honor and good name, and to make decisions about their personal life. There is also a set of legal protection measures regarding the protection of the right to privacy provided for in the provisions of the Polish Constitution. First, according to Art. 77, everyone has the right to compensation for the damage caused by an unlawful act of a public authority, and statutory law may not prevent anyone from seeking the infringed rights or freedoms. Second, according to Art. 78, each party has the right to appeal judgments and decisions issued in the first instance. Third, in accordance with Art. 79, everyone whose constitutional freedoms or rights have been violated has the right to lodge a complaint with the Constitutional Tribunal, and the court or public administration body will adjudicate his/her freedoms or rights or about his obligations set out in the Polish Constitution. Fourth, according to Art. 80 of the Polish Constitution, everyone has the right to apply to the ombudsman for assistance in the protection of their freedoms or rights infringed by public authorities, in accordance with the provisions of the Act. In light of Art. 31(3) of the Polish Constitution, there is a possibility of introducing limitations to the right to privacy, but they must be established only by statute and only if they are necessary in a democratic state for its safety or public order, or for the protection of the environment, health and public morality, or freedom and the rights of others. These restrictions must not infringe the essence of the right to privacy.

The right to privacy in civil law in Poland is mainly the Act of April 23, 1964—the Civil Code. Pursuant to Art. 23 of the Civil Code, human personal rights—in particular, health, freedom, honor, freedom of conscience, name or pseudonym, image, privacy of correspondence, inviolability of the home, and creative freedom, whether scientific, artistic, or inventive—remain under the protection of civil law, regardless of protection provided for in other regulations. Personal rights are values recognized by a legal system that encompasses the physical and mental integrity of a human being, as they are attributes of every natural person with whom they are closely related, and as such have an individual character and are protected by the construction of absolute rights. In accordance with the relevant case law, the open catalogue of personal rights also includes personal rights related to the sphere of private and family life and of intimacy. Protection in this respect may relate to cases of disclosure of facts from personal and family life, abuse of information obtained, collecting information and assessments from the sphere of intimacy through private interviews to publish them or otherwise disseminate them.

54 See Wielec, 2017.

In Poland, civil law remedies are gaining popularity due to their effectiveness. This effectiveness is high when it comes to the realities of the traditional world. However, it is different in the digital reality. The analysis presents three big problems here. The first problem is the widespread anonymity of cyberspace users. Therefore, if someone violates the privacy of another person in cyberspace, to effectively benefit from the legal protection provided for in civil law, it is necessary to establish the personal data of the infringer. In this context, the current possibilities of information, communications, and technology (ICT) detection techniques are wide, although unfortunately not very common. Thus, a possible solution to this problem could be not only to provide civil courts with the power to effectively abolish the anonymity of cyberspace users, but also to make the public aware of this fact. The second problem is the difficulty in determining the law applicable in the event of violating someone's privacy in cyberspace. We are talking here about the application of legal meta-norms, which would clearly indicate, for the benefit of the weaker party, the principles of establishing an appropriate legal system under which one can assert one's rights. In the age of digitization, this is a big problem, because the person who violates privacy may be from Canada, and the person whose privacy is violated may be from Portugal. In turn, to make things even more complicated, the breach of privacy takes place on a social network registered in the Dominican Republic. The remedy for this problem would be to define common rules for determining the applicable law. The third problem related to the second is the difficulty in determining jurisdiction in cyberspace. This difficulty is due to the same reasons as the problem of the applicable law. The solution to this problem would also be to define common rules for determining proper jurisdiction.

The right to privacy in criminal law—which is natural—has a completely different context and meaning than in civil law. Here, human privacy is protected based on penalizing violations of a legally protected good. This means that legal remedies in criminal law are specific types of prohibited acts. In turn, procedural criminal law plays a role that enables the fulfillment of the purpose of a specific legal protection measure of Polish criminal law. In Poland, the basic legal acts in this area are the Criminal Code (CC) and the Code of Criminal Procedure (CCP). In this way, in Poland, as in most modern countries, we can distinguish between substantive criminal law and procedural criminal law.

There are several types of prohibited acts in Polish substantive criminal law, which can be associated with the pursuit of repressive protection of human privacy. The basic and most important provision of Art. 267 of the CC. Other provisions of the CC, which can also be qualified as aiming at repressive protection of human privacy, are Arts. 268 (obstructing the reading of information), 268a (destruction of IT data), 269 (damage of IT data), 269a (disruption of a computer system), 269b (generation of inappropriate computer programs) and 270§1 (material forgery). The author points out that when assessing these provisions of Polish substantive criminal law from the perspective of legal protections of privacy in cyberspace, there is modern law in this area in Poland, mainly due to the good implementation of the Council of Europe Convention on Cybercrime.

There are many guarantees of respect for human privacy in Polish procedural criminal law because, as part of the criminal process, there are numerous restrictions on the rights and freedoms provided for in the Polish Constitution, especially the right to privacy. This seems to be the natural effect of Polish criminal proceedings, and thus, as a rule, of establishing the legal liability of the accused for the alleged offense. This determination often requires, even as part of evidence proceedings, state interference with the rights and freedoms of persons—the right to privacy in particular. This interference causes a normative restriction of the scope of the right to privacy, and thus reduces the protection of privacy, which means that more designations of the private sphere of a person, than under non-criminal-procedural conditions, are transferred to the public sphere.

The right to privacy, therefore, is not an absolute right and is subject to limitations, but in strict accordance with Art. 31 §1 of the Constitution. The CCP provides for rules governing the taking of evidence of a search, which provide for guarantees of respect for privacy in Art. 220 (search of an authorized body), Art. 221 (search hours), Art. 223 (search of a person), Art. 224 (method of conducting the search). Art. 227 of the CCP is of great importance here, according to which the search should be carried out in accordance with the purpose of this activity, with moderation, and within the limits necessary to achieve the purpose of these activities with due diligence, respecting the privacy and dignity of the persons concerned, and without causing unnecessary damage. The CCP also provides for provisions on the control and recording of conversations, where there are also certain guarantees of respecting human privacy. They take place in Art. 237 (conditions of application, authority, controlled entities, playback of records), Art. 238 (maximum inspection period) and Art. 240 (complaint). In terms of the protection of the essence of the right to privacy, the prohibitions on evidence, in particular in Art. 178 (prohibition of questioning the defense counsel and the clergyman), Art. 182 (right to refuse to testify), Art. 185 (exemption from the obligation to testify of a person who is in a particularly close personal relationship with the accused), and Art. 199 (secret expert information, privacy in providing medical assistance) are of great significance.

The legal norms cited above relate to the taking of evidence. Here, in terms of privacy protection, it is about maintaining the proportion between two important goods—the realization of the value of truth, and the protection of the privacy of every human being. Criminal proceedings are aimed at establishing the legal liability of the accused for the alleged offense, and for this purpose, evidence is collected, including electronic evidence.

This possibility results directly from Arts. 218a and 236a of the CCP. Therefore, data related to the needs of criminal proceedings is processed here. Referring to the usefulness and importance of legal measures to protect human privacy in Polish criminal proceedings, the appropriate rules for the processing of data obtained as evidence need to be defined. Such a need existed, as the Act on the protection of personal data processed in connection with the prevention and combating of crime was passed in Poland in 2018. The most interesting from the point of view of the title

issue are the provisions of Art. 50 (complaint against unlawful processing of personal data or notification of a violation of the processing of personal data), Art. 51 (complaint to the administrative court against the decision of the president of the office, or his/her inactivity in a complaint against the unlawful processing of personal data or reporting a violation of personal data processing), Art. 52 (authorization of a social organization to exercise rights related to the protection of personal data), and Art. 53 (compensation or compensation due from the administrator). The Act of December 14, 2018 and the presented provisions of the CCP seem to be adequate protection of human privacy based on criminal procedural law in the digital age.

The right to privacy in administrative law concerns the protection of personal data. The protection of personal data is one of the pillars of privacy protection. Poland, like most European countries, is an EU member state. Under EU law, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 was adopted on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, or GDPR) and Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by union institutions, bodies, and offices and the free movement of such data and repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002/EC. In Poland, however, one can speak of a specific national, although due to the GDPR's limited approach to the protection of personal data. This is because the Act of May 10, 2018, on the protection of personal data. Legal measures contained in constitutional, civil, criminal, and administrative law should generally be assessed positively as passing the test of legal protection of human privacy. Apart from the indicated problems, their significance and usefulness in the digital age should also be assessed positively. Nevertheless, a certain observation arises regarding the effectiveness of national law. This efficiency within the boundaries of statehood in the traditional world is at an appropriate level. On the other hand, in the digital world, without state borders and with universal anonymity, it seems that the effectiveness of national law is lower than that of common law in other countries. This is most visible in situations where the entity responsible for the right to privacy is an entity, such as transnational corporations or a social media manager. It therefore seems that international cooperation is the key to fighting for human privacy in the digital age.

## 4. Conclusions

The analysis presented showed that the right to privacy is an extremely important and topical issue. The study of its scope, content, and significance will yet take a long time ahead. The phenomenon is privacy as such, as well as the issue of delineating its boundaries and potential factors influencing or even limiting

privacy. The backbone of the right to privacy is privacy, which is very difficult to attribute to a permanent nature. It is a dynamic concept and very susceptible to environmental conditions in which this concept operates, i.e., it is about cultural, social, and even ideological circumstances and influences. The changeability of the environment in which privacy functions is what makes privacy and the right to privacy dynamic, which makes it difficult to define. Currently, one of the factors influencing the understanding of the right to privacy, characteristic of our times, is the issue of modern technologies, which, on the one hand, may support the protection and implementation of the right to privacy, and, on the other hand, may limit, interfere with, or eliminate even this right. This is a positive invention dilemma. If we assume that the invention is a new, original, technical or organizational solution of a utility character, the creation of which has the features of a creative act (in which it differs from a discovery, which is a statement of something that exists objectively), modern technologies, as a collective term, undoubtedly fit into the concept of invention.[55] The invention is often associated positively, because it most often appears as a response to current challenges, where the goal is to increase human capabilities, facilitate life and make it more comfortable, etc. In this context, modern technologies, which at first glance—as a new invention of humanity—should only bring benefits to society, but they also bring huge threats, especially in the area of privacy, broadly understood. They can be used aggressively against the community, while at the beginning of the development of these technologies there were lofty ideas for improving the life of the society. Therefore, privacy itself in the era of new inventions, methods of communication, social media, increasing the importance of datasets, is experiencing a huge renaissance. Therefore, the dilemma of a positive invention is a situation in which the emergence of anything determines both the benefits and threats. It is a situation in which, under the cover of positive expectations and effects, comfort and, at the same time, discomfort arise. Today, there is no doubt that the aforementioned renaissance of the right to privacy has its source in the dynamics of the development of human society, in its maturation that humanity, including the individual, needs a free area for its life. Currently, the key development factor is undoubtedly modern technologies that have revolutionized the approach to privacy and at the same time defined the need to define the scope of the right to privacy. It is the new technologies that are this positive invention. Modern technologies will not only facilitate the life of the community, but will also interfere with it, as a result of which there may be violations, e.g., privacy. Privacy belongs to a set of values, and thus to the circle of valuable and worthy ideas that constitute the core of the community, for which the community strives, because they are the subject of special care on the part of individuals and constitute an important goal of individuals' aspirations. Privacy as a value related to the functioning of an individual in society must therefore be protected. And since one of the functions of

55 "Invention" [Online]. Available at: https://encyklopedia.pwn.pl/haslo/wynalazek;3998913.html (Accessed: June 1, 2022).

the law is the protection of the individual, then the individual's right to privacy becomes an element of this protection. There must be some compatible privacy protection system in the form of the right to privacy of every individual, containing appropriate instruments that actually implement this protection.

The analysis showed that in virtually every country whose legal system was analyzed in terms of the right to privacy, this protection is provided by legal regulations of the highest order, i.e., by constitutional provisions. Moreover, it is right, because placing the right to privacy into constitutional provisions makes this issue itself a constitutional element. And this already proves the importance of the issue, because the constitution, as a basic law defining the foundations of the system of a given state, including regulations on the privacy of an individual, places this issue as one of the essential elements of the state system. Ensuring the right to privacy in constitutional provisions is the highest recognition of this issue in the systemic area of the state. Of course, the constitutional regulation regarding the right to privacy is characterized by a certain degree of generality, because it is the basis that delineates universal directions of this law, which is later detailed in individual legal acts of lower rank. Based on the research conducted, this is exactly what is happening. Therefore, supplementary and detailed regulations on the right to privacy in the further part of the hierarchy of legal acts can be found, *inter alia*, in acts such as the Civil Code, the Penal Code, or a number of acts relating to personal data, for example.

In addition to the noticeable model of protection of the right to privacy, the analysis carried out showed that there are several issues that future legislation should consider.

Among other things, such an issue is the right to one's image. There is no doubt that image is an inseparable component of privacy. One's image relates to the visible, physical features of a human being, which make up one's appearance and allow for identification. The image, apart from external physical features, may include additional elements related, for example, to his or her profession, such as characterization, clothing, and ways of moving and communicating with the environment.[56] These are all clearly elements of privacy that must be protected, especially if the context of the image may be ambiguous. This element of privacy, which is the image, can be used in various situations and on various occasions. However, it is always part of the right to privacy that must be fully respected.

Another issue related to the right to privacy that arose during the study was the issue of linking the norms of substantive law (e.g., civil law, criminal law) with the norms of formal law (civil proceedings, criminal proceedings) in the context of the right to privacy. While the issue of the right to privacy in substantive law is, *inter alia*, the definition of the right to privacy is already formal law (procedural law) associated with the taking of evidence. Defining the relationship between substantive law and formal law does not cause any problems, as it has been clear for years that formal law (procedural law) is the implementer of the norms of substantive law. In other words, the provisions of substantive law are triggered and implemented by the provisions of formal law.

56 Judgment of the Supreme Court dated November 10, 2017, file ref. act: V CSK 51/17.

For example, if the substantive law, e.g., the Civil Code, provides for the protection of privacy in the form of protection of one's good name (personal rights), then the implementation of this protection, i.e., a statement that there has been a violation of privacy by the violation of one's personal rights (insults, defamation) takes place by way of evidence, which is part of formal law (legal procedure): classical evidence (e.g., a witness) or modern evidence, e.g., related to the broadly understood law of new technologies. There is a clear need for the legal regulation of formal standards of digital evidence. On the other hand, the issue of creating separate courts to investigate possible breaches of the right to privacy remains to be considered. This also implies the possible formulation of specialized but very simple to apply privacy infringement actions. The construction of such claims must be simple and quick. Currently, respecting the right to privacy is most often associated with personal rights, i.e., the protection of personal rights by bringing an action for the protection of personal rights. It seems, however, that in our global society, the multitude of possible forms of privacy violations and the enormous scale of cyberspace require the creation of courts or privacy departments, and a tool to initiate and conduct such cases for the protection of privacy should be created.

In addition, the researchers in this study note several times when the right to privacy is also related to another issue that has not been discussed at all, or has been discussed only fragmentarily in the literature. Among other things, it is about the privacy of individuals who are not able to consent to interference with their privacy, especially children. Undoubtedly, this type of issue is a very important element of the right to privacy, because children, as people who only learn the rules of living in the community and as people who are essentially dependent on adults, also have their own need for privacy. The most important thing here is the family–child–parents relationship. It is a very strong and unbreakable connection. It is not without significance that the right to privacy of children should be considered in detail in national legislation.

The right to privacy is recognized as a human right and, as such, should always be effectively and rationally protected. Of course, this is not an absolute right, so exceptions to it must be justified and have strictly defined limits.

# Bibliography


Banaszak, B. (ed.) (2005) *Prawo konstytucyjne*. 3rd edn. Warsaw. C.H. Beck.

Banaszewska, A. (2013) 'Prawo do prywatności we współczesnym świecie', *Białostockie Studia Prawnicze*, 13, pp. 127–136 [Online]. Available at: https://doi.org/10.15290/bsp.2013.13.11 (Accessed: 3 June 2022).

Barth, A., Mitchell, J., Datta, A., Sundaram, S. (2007) 'Privacy and utility in business processes', *20th IEEE Computer Security Foundations Symposium (CSF'07) 2007*, pp. 279–294 [Online]. Available at: https://doi.org/10.1109/CSF.2007.26 (Accessed: 20 September 2022).

Bielecki M., Golinowski J., Kurek J., Łoszewska-Ołowska M., Mezglewski A., Oręziak B., Taczkowska-Olszewska J., Walczuk K., Wielec M. (eds.) (2021) *Zarządzanie Ludźmi w Organizacji. Zapobieganie przyczynom przestępczości*. 2nd edn. Warsaw: Instytut Wymiaru Sprawiedliwości.

Blicharz G., Oręziak B., Ratowski E., Ratowski K., Walczak P., Wielec M. (eds.) (2021) *Rynek Finansowy: Zapobieganie przyczynom przestępczości*. 2nd edn. Warsaw: Wydawnictwo Instytutu Wymiaru Sprawiedliwości.

Błasiak, A. (2018) 'Sharenting–współczesną formą rodzicielskiej narracji', *Horyzonty Wychowania*, 17(42), pp. 125–134.

Brosch, A. (2018) 'Sharenting–Why do parents violate their children's privacy?', *The new educational review*, 54(4), pp. 75–85 [Online]. Available at: https://doi.org/10.15804/tner.2018.54.4.06 (Accessed: 20 September 2022).

Bucińska, J. (2001) 'Godność człowieka jako podstawowa wartość porządku prawnego', *Państwo — Administracja — Kościół*, 2(3), pp. 32–33.

Burgoon, J. K. (1982) 'Privacy and communication', *Annals of the International Communication Association*, 6(1), pp. 206–249 [Online]. Available at: https://doi.org/10.1080/23808985.1982.11678499 (Accessed: 20 September 2022).

Bygrave, L. A. (2001) 'The place of privacy in data protection law', *University of New South Wales Law Journal*, 24(1), pp. 277–283.

Chaudhuri, A. (2016) 'Internet of things data protection and privacy in the era of the General Data Protection Regulation', *Journal of Data Protection & Privacy*, 1(1), pp. 64–75.

Choudhury, H., Roychoudhury, B., Saikia, Dilip, K. (2012) 'Enhancing user identity privacy in LTE' in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. Liverpool: IEEE. pp. 949–957 [Online]. https://doi.org/10.1109/TrustCom.2012.148 (Accessed: 20 September 2022).

Cmiel, K. (2004) 'The recent history of human rights', *The American Historical Review*, 109(1), pp. 117–135 [Online]. https://doi.org/10.1086/530153 (Accessed: 20 September 2022).

Cole, D., Fabbrini, F. (2016) 'Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders', *International Journal of Constitutional Law*, 14(1), pp. 220–237 [Online]. Available at: https://doi.org/10.1093/icon/mow012 (Accessed: 20 September 2022).

Coleman, C. (2003) 'Cyberspace security: Securing cyberspace – new laws and developing strategies', *Computer Law & Security Report*, 19(2), pp. 131–136 [Online]. Available at: https://doi.org/10.1016/S0267-3649(03)00208-5 (Accessed: 20 September 2022).

Custers, B., Uršič, H. (2016) 'Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection', *International data privacy law*, 6(1), pp. 4–15 [Online]. Available at: https://doi.org/10.1093/idpl/ipv028 (Accessed: 20 September 2022).

DeCew, J. W. (1986) 'The scope of privacy in law and ethics', *Law and Philosophy,* 1986(5), pp. 145–173; https://doi.org/10.1007/BF00190759.

Diggelmann, O., Cleis, M. N. (2014) 'How the right to privacy became a human right', *Human Rights Law Review*, 14(3), pp. 441–458 [Online]. Available at: https://doi.org/10.1093/hrlr/ngu014 (Accessed: 20 September 2022).

Dubisz, S. (ed.) (2006) *Uniwersalny słownik języka* polskiego. 1st edn. Warsaw: Wyd. Naukowe PWN.

*Encyklopedia – wynalazek* [Online]. Available at: https://encyklopedia.pwn.pl/haslo/wynalazek;3998913.html (Accessed 1 June 2022).

Feng, Q., He, D., Zeadally, S., Khan, M. K., Kumar, N. (2019) 'A survey on privacy protection in blockchain system', *Journal of Network and Computer Applications*, 2019(126), pp. 45–58 [Online]. Available at: https://doi.org/10.1016/j.jnca.2018.10.020 (Accessed: 20 September 2022).

Filiczkowska, J., Oręziak, B., Płonka, M., Szaraniec, M., Strupczewski, G., Wielec, M., Witwicka-Szczepankiewicz, A. (2021) *Rynek Ubezpieczeniowy. Zapobieganie przyczynom przestępczości*. Warsaw: Wydawnictwo Instytutu Wymiaru Sprawiedliwości.

Floridi, L. (2016) 'On Human Dignity as a Foundation for the Right to Privacy', *Philosophy & Technology*, 29(4), pp. 307–312 [Online]. Available at: https://doi.org/10.1007/s13347-016-0220-8 (Accessed: 20 September 2022).

Fox, A. K., Grubbs Hoy, M. (2019) 'Smart devices, smart decisions? Implications of parents' sharenting for children's online privacy: An investigation of mothers', *Journal of Public Policy & Marketing*, 38(4), pp. 414–431 [Online]. Available at: https://doi.org/10.1177/0743915619858290 (Accessed: 20 September 2022).

Francis, J. G., Leslie, P. F. (2018) 'Privacy, Employment, and Dignity', in Cudd, A., Navin, M. (eds.) *Core Concepts and Contemporary Issues in Privacy AMINTAPHIL: The Philosophical Foundations of Law and Justice*. Cham: Springer, pp. 207–218; https://doi.org/10.1007/978-3-319-74639-5_14.

Gardos, P. (2007) 'Recodification of the Hungarian civil law', *European Review of Private Law*, 15(5), pp. 707–722 [Online]. Available at: https://doi.org/10.54648/ERPL2007037 (Accessed: 20 September 2022).

Garmendia, M., Martínez, G., Garitaonandia, C. (2022) 'Sharenting, parental mediation and privacy among Spanish children', *European Journal of Communication*, 37(2), pp. 145–160 [Online]. Available at: https://doi.org/10.1177/02673231211012146 (Accessed: 20 September 2022).

Van Bueren, G. (1994) 'The International Legal Protection of Children in Armed Conflicts', *International & Comparative Law Quarterly*, 43(4), pp. 809–826 [Online]. Available at: https://doi.org/10.1093/iclqaj/43.4.809 (Accessed: 20 September 2022).

Goggin, G., Ellis, K. (2020) 'Privacy and digital data of children with disabilities: Scenes from social media sharenting', *Media and Communication*, 8(4), pp. 218–228 [Online]. Available at: https://doi.org/10.17645/mac.v8i4.3350 (Accessed: 20 September 2022).

Górska, A., Jankiewicz, S., Józefczyk, V., Kwiatkiewicz, P., Oręziak, B., Piekarz, D., Rosicki, R., Wielec, M., Wojcieszak, Ł. (2021) *Rynek Energetyczny. Zapobieganie przyczynom przestępczości*. Warsaw: Wydawnictwo Instytutu Wymiaru Sprawiedliwosci.

Habermas, J. (2018) 'The concept of human dignity and the realistic utopia of human rights', in Nascimento, A., Bachmann, M. (eds.) *Human Dignity, Perspectives from a Critical Theory of Human Rights*. 1st edn. London: Routledge; https://doi.org/10.4324/9781315468297-4.

HAMZA, G. (2019) 'Codification of Hungarian Private (Civil) Law in a Domestic and International Comparison', *Polgári Szemle: Civic Review, Learned Paper for Economic and Social Sciences – Hungary,* 15(Special Issue), pp. 443–450 [Online]. Available at: https://doi.org/10.24307/psz.2019.0823 (Accessed: 20 September 2022).

HANCOCK, B. (2000) 'US and Europe Cyber Crime Agreement Problems', *Computers & Security*, 19(4), p. 310 [Online]. Available at: https://doi.org/10.1016/S0167-4048(00)04016-5 (Accessed: 20 September 2022).

ISHAY, M. R. (2008) *The History of Human Rights: From Ancient Times to the Globalization Era,* Berkeley: University of California Press.

JEDLECKA, W. (2013) 'Godność człowieka jako podstawa aksjologiczna porządku prawa Unii Eu' in BATORA, A., JABŁOŃSKI, M., MACIEJEWSKI, M., WÓJTOWICZ, K. (eds.) *Współczesne koncepcje ochrony ochrony wolności i praw podstawowych*, Wrocław: Wyd. Prawnicza i Ekonomiczna Biblioteka Cyfrowa, pp. 167–177 [Online]. Available at: http://www.bibliotekacyfrowa.pl/Content/43840/014.pdf (Accessed 1 July 2022).

JENSEN, M. (2013) 'Challenges of privacy protection in big data analytics' in *2013 IEEE International Congress on Big Data*, IEEE [Online]. Available at: https://doi.org/10.1109/BigData.Congress.2013.39 (Accessed: 20 September 2022).

Judgment of the Supreme Court dated November 10, 2017, file ref. act: V CSK 51/17.

JURCZYK, T. (2009) 'Geneza rozwoju praw człowieka', *Homines Hominibus*, 2009/1, pp. 29–44.

Justification for the Judgment of the Constitutional Tribunal of April 11, 2000, file ref. Act. K. 15/98, OTK ZU No. 3 (2000), item 86.

KANTOROWICZ, H. (1958) *The Definition of Law,* Cambridge: Cambridge University Press.

KIGERL, A. C. (2009) 'CAN SPAM Act: An Empirical analysis', *International Journal of Cyber Criminology*, 3(2), pp. 566– 589.

KOOPS, B. J., LEENES, R. (2014) 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law', *International Review of Law, Computers & Technology,* 28(2), pp. 159–171 [Online]. Available at: https://doi.org/10.1080/13600869.2013.801589 (Accessed: 20 September 2022).

KUSHELVITZ, E. (1992) 'Privacy and communication complexity' *SIAM Journal on Discrete Mathematics*, 5(2), pp. 273–284 [Online]. Available at: https://doi.org/10.1137/0405021 (Accessed: 20 September 2022).

LANGOS, C. (2012) 'Cyberbullying: The challenge to define', *Cyberpsychology, behavior, and social networking*, 15(6), pp. 285–289 [Online]. Available at: https://doi.org/10.1089/cyber.2011.0588 (Accessed: 20 September 2022).

LILIEN, L., KAMAL, Z.H., BHUSE, V., GUPTA, A. (2007) 'The Concept of Opportunistic Networks and their Research Challenges in Privacy and Security' in MAKKI, S. K., REIHER, P., MAKKI, K., PISSINOU, N., MAKKI, S. (eds.) *Mobile and Wireless Network Security and Privacy*. Boston: Springer International Publishing, pp. 85–117; https://doi.org/10.1007/978-0-387-71058-7_5.

MCDOUGAL, M. S. (1959) 'Perspectives for an International Law of Human Dignity' in *Proceedings of the American Society of International Law at its annual meeting (1921-1969), 53*. Cambridge: Cambridge University Press, pp. 107–136; https://doi.org/10.1017/S0272503700023314.

MELTON, G. B., FLOOD, M. F. (1994) 'Research policy and child maltreatment: Developing the scientific foundation for effective protection of children', *Child Abuse & Neglect,* 1994(18), pp. 1–28 [Online]. Available at: https://doi.org/10.1016/0145-2134(94)90088-4 (Accessed: 20 September 2022).

Mielnik, Z. (1996) 'Prawo do prywatności (zagadnienia wybrane)', *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 58(2), pp. 29–41.

Moreham, N. A. (2008) 'Why is privacy important? Privacy, dignity and development of the New Zealand breach of privacy tort' *Victoria University of Wellington Legal Research Papers*, 5(24), pp. 231–247.

Motyka, K. (2010) 'Prawo do prywatności', *Zeszyty Naukowe Akademii Podlaskiej w Siedlcach. Seria: Administracja i Zarządzanie,* 2010(10), pp. 8–36.

Muras, Z. (2014) 'Ogólne wiadomości o prawie' [Online]. Available at: https://www.ksiegarnia.beck.pl/media/product_custom_files/1/2/12590-podstawy-prawa-zdzislaw-muras-darmowy-fragment.pdf (Accessed 5 June 2022).

Ogbuke, N. J., Yusuf, Y. Y., Dharma, K., Mercangoz, B. A. (2022) 'Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society', *Production Planning & Control*, 33(2-3), pp. 123–137 [Online]. Available at: https://doi.org/10.1080/09537287.2020.1810764 (Accessed: 20 September 2022).

Olweus, D., Limber, S. P. (2018) 'Some problems with cyberbullying research', *Current Opinion in Psychology*, 2018(19), pp. 139–143 [Online]. Available at: https://doi.org/10.1016/j.copsyc.2017.04.012 (Accessed: 21 September 2022).

Ondreasova, E. (2018) 'Personality Rights in Different European Legal Systems: Privacy, Dignity, Honour and Reputation', in Oliphant, K., Pinghua, Z., Lei, C. (eds.) *The Legal Protection of Personality Rights*, Brill Nijhoff, pp. 24–70; https://doi.org/10.1163/9789004351714_004.

Oomen, I., Leenes, R. (2008) 'Privacy risk perceptions and privacy protection strategies' in Leeuw, E., Fischer-Hübner, S., Tseng, J., Borking, J. (eds.) *Policies and research in identity management*. Boston: Springer, pp. 121–138; https://doi.org/10.1007/978-0-387-77996-6_10.

Plattner, D. (1984) 'Protection of children in international humanitarian law', *International Review of the Red Cross (1961-1997)*, 24(240), pp. 140–152 [Online]. Available at: https://doi.org/10.1017/S002086040006993X (Accessed: 21 September 2022).

Proposal for a Regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM / 2021/206 final).

Purtova, N. (2018) 'The law of everything. Broad concept of personal data and future of EU data protection law', *Law, Innovation and Technology*, 10(1), pp. 40–81 [Online]. Available at: https://doi.org/10.1080/17579961.2018.1452176 (Accessed: 21 September 2022).

Pryciak, M. (2010) 'Prawo do prywatności' in Sadowski, M., Szymaniec, P. (eds.) *Prawa człowieka: idea, instytucje, krytyka*. Wrocław: Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, pp. 211–229; [Online]. Available at: http://www.bibliotekacyfrowa.pl/Content/37379/011.pdf (Accessed: 5 June 2022).

Reidenberg, J. (2005) 'Technology and Internet Jurisdiction', *University of Pennsylvania Law Review*, 153(6), pp. 1951–1974 [Online]. Available at: https://doi.org/10.2307/4150653 (Accessed: 21 September 2022).

Rodham, H. (1973) 'Children under the law', *Harvard Educational Review*, 43(4) pp. 487–514 [Online]. Available at: https://doi.org/10.17763/haer.43.4.e14676283875773k (Accessed: 21 September 2022).

Roessler, B. (2017) 'X-privacy as a human right' *Proceedings of the Aristotelian Society*, 117(2), pp. 187–206 [Online]. Available at: https://doi.org/10.1093/arisoc/aox008 (Accessed: 21 September 2022).

Rössler, B. (2005) *The value of privacy*, Cambridge: Polity Press.

Sabella, R. A., Patchin, J. W., Hinduja, S. (2013) 'Cyberbullying myths and realities', *Computers in Human behavior*, 29(6), pp. 2703–2711 [Online]. Available at: https://doi.org/10.1016/j.chb.2013.06.040 (Accessed: 21 September 2022).

Sadowski, M. (2007) 'Godność człowieka – aksjologiczna podstawa państwa i prawa', *Wrocławskie Studia Erazmiańskie*, 2007/1. pp. 8–28.

Saria, V. (2022) 'Differs in Dignity: Shame, Privacy, and the Law' in Vakoch, D. A. (ed.) *Transgender India*. Cham: Springer, pp. 99–116; https://doi.org/10.1007/978-3-030-96386-6_7.

Shapiro, A. L. (1999) 'The Internet', *Foreign Policy*, 1999/115. pp. 14–27 [Online] Available at: https://doi.org/10.2307/1149490 (Accessed: 21 September 2022).

Simon, G. E. (1997-1998) 'Cyberporn and Censorship: Constitutional Barriers to Preventing Access to Internet Pornography by Minors', *The Journal of Criminal Law and Criminology*, 88(3), p. 1015–1048 [Online]. Available at: https://doi.org/10.2307/3491360 (Accessed: 21 September 2022).

Skorowski, H. (2003) 'Prawa człowieka' in Zwoliński, A. (ed.) *Encyklopedia nauczania społecznego Jana Pawła I, Radom*. Polwen.

Skrzydło, W. (2005) *Polskie prawo konstytucyjne*. Lublin: Verba.

Slonje, R., Smith, P. K., Frisén, A. (2013) 'The nature of cyberbullying, and strategies for prevention', *Computers in Human Behavior*, 29(1), pp. 26–32 [Online]. Available at: https://doi.org/10.1016/j.chb.2012.05.024 (Accessed: 21 September 2022).

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., Tippett, N. (2008) 'Cyberbullying: Its nature and impact in secondary school pupils', *Journal of child psychology and psychiatry*, 49(4), pp. 376–385 [Online] Available at: https://doi.org/10.1111/j.1469-7610.2007.01846.x (Accessed: 21 September 2022).

Sobczyk, P. (2017) 'Ochrona danych osobowych jako element prawa do prywatności' *Zeszyty Prawnicze*, 9(1) pp. 299–318 [Online]. Available at: https://doi.org/10.21697/zp.2009.9.1.14 (Accessed: 21 September 2022).

Spiekermann, S. (2012) 'The challenges of privacy by design', *Communications of the ACM* 55(7), pp. 38–40 [Online]. Available at: https://doi.org/10.1145/2209249.2209263 (Accessed: 21 September 2022).

Stolz, B. A. (1983) 'Congress and Capital Punishment: An Exercise in Symbolic Politics', *Law & Policy*, 5(2), pp. 157–180 [Online]. Available at: https://doi.org/10.1111/j.1467-9930.1983.tb00294.x (Accessed: 22 September 2022).

Sut, P. (2000) 'Ochrona godności człowieka a tzw. nowe media', *Gdańskie Studia Prawnicze*, 7, p. 525.

Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018) 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies', *Computer Law & Security Review*, 34(1), pp. 134–153 [Online]. Available at: https://doi.org/10.1016/j.clsr.2017.05.015 (Accessed: 22 September 2022).

Trepte, S. (2021) 'The Social Media Privacy Model: Privacy and Communication in the Light of Social Media Affordances', *Communication Theory* 31(4), pp. 549–570 [Online]. Available at: https://doi.org/10.1093/ct/qtz035 (Accessed: 22 September 2022).

Van Bueren, G. (1994) 'The International Legal Protection of Children in Armed Conflicts', *International & Comparative Law Quarterly*, 43(4), pp. 809–826 [Online]. Available at: https://doi.org/10.1093/iclqaj/43.4.809 (Accessed: 22 September 2022).

Walden, I. (2004) 'Harmonising Computer Crime Laws in Europe', *European Journal of Crime, Criminal Law and Criminal Justice*, 12(4), pp. 321–336 [Online]. Available at: https://doi.org/10.1163/1571817042523095 (Accessed: 22 September 2022).

Wermiel, S.J. (1998) 'Law and human dignity: The judicial soul of Justice Brennan', *Wm. & Mary Bill Rts. J.*, 7(1), p. 223–239.

Whitehead, J., Wheeler, H. (2008) 'Patients' experiences of privacy and dignity. Part 1: a literature review', *British Journal of Nursing*, 17(6), pp. 381–385 [Online] Available at: https://doi.org/10.12968/bjon.2008.17.6.28904 (Accessed: 22 September 2022).

Wible, B. (2003) 'A Site Where Hackers are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime', *The Yale Law Journal*, 112(6), pp. 1577–1623 [Online]. Available at: https://doi.org/10.2307/3657453 (Accessed: 22 September 2022).

Wielec, M., Oręziak, B. (2021) 'Transforming People and Organizations: Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości w kontekście implementacji najnowszych rozwiązań prawnych i organizacyjnych' in Koszewski, R., Oręziak, B., Wielec, M. (eds.) *Wdrożenie metod i instrumentów zapobiegania przestępczości w organizacjach.* Warsaw: Instytut Wymiaru Sprawiedliwości, pp. 113–139.

Wielec, M., Oręziak, B. (2020) 'Assessing Foundations: Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości w kontekście zidentyfikowania problemu przestępczości w Polsce i na świecie' in Koszewski, R., Oręziak, B., Wielec, M. (eds.) *Identyfikacja przyczyn przestępczości w wybranych obszarach gospodarki w Polsce i na świecie*. Warsaw: Wydawnictwo Instytutu Wymiaru Sprawiedliwości, pp. 121–147.

Wielec, M., Oręziak, B. (2020) 'Heading Into the Future: Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości w kontekście przyszłości i przyszłych zmian' in Koszewski, R., Oręziak, B., Wielec, M. (eds.) *Identyfikacja przyczyn przestępczości w wybranych obszarach gospodarki w Polsce i na świecie*. Warsaw: Wydawnictwo Instytutu Wymiaru Sprawiedliwości, pp. 117–140.

Wielec, M. (2017) *Wartości – Analiza z perspektywy osobliwości postępowania karnego.* Lublin: Wydawnictwo Academicon.

Wielec, M., Oręziak, B. (2021) 'Improving Performance. Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości w kontekście metodyki' in Koszewski, R., Oręziak, B., Wielec, M. (eds.) *Metody zapobiegania przestępczości*. Warsaw: Wydawnictwo Instytutu Wymiaru Sprawiedliwości, pp. 101–127.

Williams, M. A. (2009) 'Privacy management, the law & business strategies: A case for privacy driven design', *2009 International Conference on Computational Science and Engineering, IEEE*, pp. 60–67 [Online]. Available at: https://doi.org/10.1109/CSE.2009.478 (Accessed: 06 October 2022).

Witkowski, Z. (ed.) (2001) *Prawo konstytucyjne*. 9th edn. Torun: Dom Organizatora.

Wojciechowski, B. (2009) 'Interkulturowe prawo karne. Filozoficzne podstawy karania w wielokulturowych społeczeństwach demokratycznych', *Państwo i Prawo*, 65(10), pp. 126–129.

Chapter II

# The Right to Privacy in the European Context: Insight into Fundamental Issues

Vanja-Ivan Savić

## 1. Introduction

To write on the right to privacy in the 21st century is to undertake a multidimensional task, one that can be approached from the perspective of both the contemporary citizen and the jurist in several distinct ways. We live at a time when our need for private space is sought more vigorously than the air we breathe, inhabiting a technological world saturated with cameras, gadgets, telephones, TVs and CCTVs; in short, a world where information has become the most important and most expensive feature. Quick information is essential, and the holders of such information tend to be powerful and well equipped. People and places are valued by technological and social media appearance; it is impossible to measure the level of voyeurism we are all enmeshed in. Real values – values of having your private space for yourself, for family and family life, and the right to be a functional human in the dehumanized world of wires and screens – seem to be urgently and fundamentally relevant.

Yet, the reality of modern life requires that the State, the principal guarantor of peace and freedom, provides a functional, safe and secure life for everyone. To do this, States use the same technological tools; screens, cameras, CCTVs, computers and telephones. Thus, from a philosophical – or even meta-philosophical – aspect, the protection of privacy is simultaneously a blessing and a curse. How

Vanja-Ivan Savić (2023) The Right to Privacy in the European Context: Insight into Fundamental Issues. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 47–75. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_2

does one resolve such fundamental tensions? The key to the solution lies, like in many other things, in *balancing*. I have learned that balancing became one of the major tools in tranquilizing and confronting rights, especially on the European continent. This chapter will thus focus on the European continent; I will examine selected topics on privacy primarily through the ECHR and the decisions of the court. A secondary method of investigation will be historical and analytical, and will attempt to answer such questions as what privacy really means and what the origins of Privacy Law are. As in many other areas of legal regulation, the State needs to clarify at least three facts: (1) what the highest values of the respective legal order are as per the Constitutional Law and Hierarchy of Norms; (2) what the priorities, through level of protection, are; and (3) whether the 'not to harm principle' has been applied. This essentially ensures that by protecting one right, the rights of others will not be endangered; such results are achieved by balancing. Each State has to decide which are the most important values if the society which make fundaments of its existence. This paper will primarily focus on fundamental values which have to be protected through Privacy Law, as well as some basic aspects of privacy: privacy of family life, privacy of religious organizations, and protection of religious freedoms. An important section will be dedicated to privacy in private life and to data protection (mostly GDPR). All these topics are connected to the core values common to European society as a whole. However, some additional attention will be given to the Central and Eastern European countries and their values.

Obviously, the central clash is between private and family life on the one hand and security on the other. Therefore, the balancing act should be attempted with a clear sight of the values and the public order of a particular State. Moreover, the Margin of Appreciation doctrine should also be taken into account. For instance, religious places of worship have to be excused from surveillance and respected as a sacred space, but at the same time security issues and safety protocols have to be taken into account and properly balanced. At this point it is important to secure and fully respect the application of human rights standards which are essential for the perception of the contemporary European lawyer and citizen.

Recently, another modern privacy issue arose with the onset of the Covid-19 pandemic. In the beginning, no one really thought that a pandemic could also be privacy issue, but it turned out that epidemiological regulation affects private life and religious freedoms much more than anticipated. Private life is potentially endangered through the requirement of masks and vaccinations. The new pandemic brought fort several global challenges. In sum, this paper will act as a contemplative text about privacy in the European context, with specifically chosen topics arising from the legal discourse on privacy.

## 2. Origins of privacy in Europe (European Union and the Council of Europe)

Although under the Treaty on the Functioning of the European Union (Lisbon Treaty), which entered into force on December 1, 2009, and where the protection of *personal data is recognized as a fundamental right,* most issues related to the right to privacy in the legislation of the European Union are concerned with legal entities and business activities which overflow into various private and non-corporate sectors. This is the case with the GDPR. Although the majority of the analysis in this article will be connected with the activity of the European Court of Human Rights, there is a real necessity to mention two basic pillars important for the development of European legislation[1]:

- Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (the "Data Privacy Directive")
- Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (the "E-Privacy Directive")

In the corporate world we live in today, most people, several scholars included, first think of Privacy Law as 'corporate privacy' or the GDPR. However, the history of privacy laws goes much deeper and is linked to individual privacy rights or privacy expectations, for example, the right to have private and undisturbed life. How this

1 EU data privacy laws, EU Treaties and Charters, Legal Information Institute, Cornell University [Online] Available at: https://www.law.cornell.edu/wex/eu_data_privacy_laws (Accessed: 23 February 2022). An excellent summary is provided by the Cornell's LII: "The Data Privacy Directive established the basic legal framework for data privacy protection in the EU, including the default requirement of "opt-in" consent to data sharing and the "adequacy requirement" for data-sharing with non-EU companies. In response to this latter requirement, the U.S. negotiated a "safe harbor" framework for U.S. companies doing business in Europe or with European companies. The Data Privacy Directive also reflects the basic principle that EU privacy protections must be balanced against the four "fundamental freedoms" of the European "internal market": free movement of persons, goods, services, and capital. The E-Privacy Directive supplements the Data Privacy Directive, replacing a 1997 Telecommunications Privacy Directive, and providing a minimum standard for EU member state regulation of commercial solicitation by means of email and telecommunications technologies. It has specific provisions regarding unsolicited communications. Article 13 of the E-Privacy Directive sets forth a basic rule of "opt-in" consent for "unsolicited communications": automated telephone calls, faxes, texts, and email. With respect to unsolicited commercial emails, an exception is created in Article 13(2) for cases where a business has provided a good or service to an individual previously, the individual has provided his/her email, and an unsolicited email is sent to advertise "similar" goods or services. Unsolicited emails sent under this exception must, however, provide the customer with an opportunity to "opt-out" of future emails. Article 13(4) prohibits the sending of commercial emails that disguise or conceal the identity of the sender. See also European Commission Website: Unsolicited Communications – Fighting Spam."

is important? The pure fact remains that this right has its foundation in the Universal Declaration of Human Rights talks by itself. In its Article 12, the UDHR states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[2] In a wonderful article two Swiss scholars Oliver Diggelmann and Maria Nicole Cleis argue that the right to privacy was and therefore still is a 'human right', even before it became a 'well-established fundamental right'.[3] This is particularly important to bear in mind when we discuss rights of individuals and/or communities. It is important to go back to the roots of the institution and seek answers to complicated questions which have arisen later on in its development. Privacy concerns are thus much 'older' than we might first think.

It is interesting to note that prior to the Second World War (WWII) European constitutions didn't recognize 'privacy' or 'right to privacy' as a constitutional right – and even then, very few references to 'privacy' have been shown, for example, the correspondence or inviolability of home.[4] General guarantees, as said, were non-existent. The issue is that human rights are the essence of fundamental rights in every liberal State constitution.[5] As the Swiss authors succinctly put it, the usual manner of evolution of rights is such that those that are present significantly at the national level in time become the instrument of conventional law.[6] A definition of the right to privacy does not exist and in that sense belongs to those definitions which have a large impact and define much, but without the definition in itself existing, like the case is with law, or dignity or honesty for instance.[7]

> Privacy is about creating distance between oneself and society, about being left alone (privacy as freedom from society), but it is also about protecting elemental community norms concerning, for example, intimate relationships or public reputation (privacy as dignity). These core ideas compete and partially even contradict each other.[8]

Most scholars do agree that there were two reasons why the right to privacy jumped so high in conventional law; first, the development of electronic or digital media and human development, but the catchment of the institution were undermined when it was created. It has been proven that privacy became present on all levels of legal regulation. However, it has to be remembered that privacy was

2 Universal Declaration on Human Rights [Online] Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed: 23 February 2022).
3 Diggelmann and Cleis, 2014, pp. 441–458.
4 Ibid. p. 441.
5 Ibid. p. 442.
6 Ibid.
7 See Warren and Brandeis, 1890, p. 193; Solove, 2002, p. 1087; Griffin, 2007, p. 697.
8 See Diggelmann and Cleis, 2014, p. 442.

conventionally set up in the UDHR in its Art. 12 which became a corner stone and legal standard for all regulation in the area of privacy law.

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[9]

The document which was produced at that stage was named a Declaration, while there were attempts to make a convention rather than a manifest. At that stage of history (post WWII) it was obviously much easier to get a compromise or agreement on something which is more legally soft or which looks like a moral norm in its essence. Nevertheless, the impact of such a document still remains far greater than just a pure text of good wishes.[10] When we observe the development of privacy law historically, regulations progressed in a few different directions and what was meant to be protected foremost was privacy, private life and family.

In the second phase of the drafting, the wording was that 'everyone is entitled to protection under the law from unreasonable interference with reputation, family, home or correspondence'[11], which was significant since family and home became more focal. There were discussions on if family should have a guarantee to be 'protected from interference' or a guarantee to have 'freedom from interference'[12]. Although there were obvious differences in approaches and wordings, sometimes more than just linguistic differences, all agreed that family and home should be specially protected. Therefore it is not wrong to state that one of the most important aspect of privacy is connected with family life and the privacy of home, which has to be further connected with contemporary issues related to the protection of family, family values and the right to educate children according to specific morals and worldviews. Moreover, there are links with issues of religious freedom. Correspondence also became important as we encounter questions of uninterrupted communication. Surveillance exists in many aspects of private life, and private communication can be interrupted by technical means. This also has implications for organizational religious freedom, which will be discussed later in the text.[13] Communication and correspondence does not mean only classical writings but more importantly includes

9 Universal Declaration on Human Rights [Online] Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights, (Accessed: 25 February 2021).

10 See Diggelmann and Cleis, 2014, pp. 443–444., and also Universal Declaration on Human Rights [Online] Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights, (Accessed: 25 February 2021) referral to: Commission on Human Rights, 2nd Session, Summary Record of the 28th Meeting, 4 December 1947, E/CN.4/SR/28 ('Commission Summary Record 28').

11 Diggelmann and Cleis, 2014, p. 446.

12 Diggelmann and Cleis, 2014, p. 447. Cit: "The discussions in the Committee focused on whether to include family rights or not and on whether the provision should be designed as a guarantee to 'protection from interference' or as a guarantee to 'freedom from inference'. 'Protection' implies more duties for the State than the obligation to respect the freedom from interference."

13 See supra.

all modes of private interaction including the use of the internet and social media. Of course, given how it is set up in Art. 12 of the UDHR, the State has control over privacy ('no one shall be subjected to arbitrary interference'), which makes correctional pre-clause and ensures that interference with privacy is and should be in accordance with law. There are different solutions regarding the scope of state control and the scope and limits of protected values, but this wording secures the most important thing; balancing. Balancing will be the most important mechanism to secure equal legal presence of private life on the one hand and necessary state control on the other. Although the flavor of the text has a clear influence of Anglo-American vocabulary, the clause remains clear and understandable to members of all legal systems.

There are also other documents which cover the right to privacy like the Covenant on Civil and Political Rights, which was set up through Art. 17:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.[14]

In this article of the ICCPR, the same rights are protected and this has to be taken into account when discussing the scope of protection through privacy law. This is shaped by the fact that privacy, family, home and correspondence are connected with honor and reputation. It is important to notice that since the ICCPR, as one of the key documents, the intention begun to also protect honor and reputation through the private sphere. Later on, this process will be elevated to protection through criminal law. All in all, privacy has to be tested thorough the reputation and/or honor test.

## 3. Declaration on human dignity for everyone everywhere

One of the most important documents of the 21st century is the one which was signed in Punta Del Este in Uruguay in December 2018, the Punta Del Este Declaration of Human Dignity for Everyone Everywhere, which reaffirms the UDHR.[15] The Declaration on Human Dignity was made as a reflection on the 70th Anniversary

14 International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Art. 49 [Online] Available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (Accessed: 28 February 2022).

15 Punta del Este Declaration on Human Dignity for Everyone Everywhere [Online] Available at: https://www.dignityforeveryone.org/introduction/ (Accessed: 3 March 2022).

of the UDHR. The core value of this Declaration is that it reaffirms positions which existed and had been derived from the UDHR, but set up more on the concept of human dignity which emphasizes the source of the right of others, which is the core of humanity, in all directions, for all. It also stated that human rights involve corresponding duties. This means that the minority has to be treated well and with respect, but also that the minority should respect majority. Dignity as a source of human rights requests that all views should be taken into account, including the rights of groups or societies from diverse worldviews, but with the understanding of the essence of public morals and *ordre public,* as well as the reasons for why one society looks different from another. For example, surveillance might not be acceptable in religious premises, but if the religious community threatens public order and peace, it might be acceptable. It might be useful, from the perspective of security, to record the voice of a particular person, but it might be crossing the line if the recording catches, for instance, members of the whole family. Therefore in both cases the dignity of the person will be examined and balanced with the particular social values of a particular society. This could be called the *public order test* or the test of public order.

Therefore, we have to approach law as a reflection and summary of the beliefs and moral values of a majority of citizens who, by the power of their original and genuine rights, transfer the capacity of making law to representatives that will bound themselves and the nation itself. This is called the democratic principle. Of course, in every decent democracy the majority has to find a way to respect different needs, creeds and attitudes to the maximal possible limit in order not to break the core values of the society in question. This is called the human rights principle. A just society, in my view, is one that tries to achieve the right balance between the two.[16] It is this balancing that secures all rights and values equally (in its nature) and ensures that they are well regarded. This is underlined in the Declaration on Human Dignity:

> Human dignity for everyone everywhere emphasizes the concept in the UDHR that rights include accompanying obligations and responsibilities, not just of states but also of all human beings with respect to the rights of others. Dignity is a status shared by every human being, and the emphasis on everyone and everywhere makes it clear that rights are characterized by reciprocity and involve corresponding duties. Everyone should be concerned not only with his or her own dignity and rights but with the dignity and rights of every human being. Nonetheless, human dignity is not diminished on the ground that persons are not fulfilling their responsibilities to the state and others.[17]

16 See Savić, 2016, p. 679.

17 Punta del Este Declaration on Human Dignity for Everyone Everywhere [Online] Available at: https://www.dignityforeveryone.org/introduction/ (Accessed: 3 March 2022).

> Recognition of human dignity for everyone everywhere is a foundational principle of law and is central to developing and protecting human rights in law and policy. The richness of the concept of dignity resists exhaustive definition, but it encourages the pursuit of optimum mutual vindication where conflicting rights and values are involved. It is critical for moving beyond thinking exclusively in terms of balancing and tradeoffs of rights and interests.[18]

Why is this Declaration so important? In recent years, at least in Europe, public space legal discourse of human rights has largely been shaped in a way that suits the stance and positions of those espousing left and liberal positions on the political spectrum. For such trends, blame must also be assigned to conservative and demagogic Christian parties and policies which have allowed the identification of human rights with new tendencies and cultures that have been developing in the contemporary world. Spiritual laziness allowed the hyper concentration of concept(s) which only underline a few sub-groups of human rights and present them as the core of the human rights movement, or rather present them as 'Human Rights' as such. From this perspective, human rights are only connected with so called progressive movements and one easily forgets that the roots of human rights as we know them today lie in the documents which were written under influences of moral philosophy (and also politics) which included, *inter alia,* Christian and 'conservative' values. The UDHR, the key document of mankind, was influenced, for instance, by Lebanese Charles Habib Malik, a Christian who insisted on the protection of family values, and his work is a reflection of his belief that people have a spiritual dimension and that family is important.[19]

The crucial notion on dignity lies in its relation to human rights. Most scholars[20] agree that human rights are products or derivatives of human dignity. In other words, human dignity is a source of human rights and as such holds a very special position. Human dignity is more than just a legal standard – it is a specific legal foundation that guarantees every human a special, non-infringed position towards all people in their integrity, and a genuine right to have and live their own values. It also grants protection for his or her living space. Therefore understanding human dignity is important to understand space, which belong to every person as free men. This is obviously connected with privacy and privacy law which protects the whole personality of the individual and his private life. *It would be essential to understand*

18 Ibid. at. 7 'Implementing and Realizing Human Rights in Legislation'.

19 Savić, 2019, p. 175.: "It is not so well known that as an Orthodox Christian he wrote one of the most valuable books published in the Middle East after WWII which reflects his ideas at the time when the Universal Declaration of Human Rights was signed. In Christ and Crisis, first published in 1962 (newly reprinted by Acton Institute (Grand Rapids, MI, USA) in 2015), Malik states that the deepest crisis of our age is a spiritual one which, in his view, is clearly recognized and underlined by the Church. He was a devoted Christian and was heavily involved in ecumenical work."

20 See Punta del Este Declaration on Human Dignity for Everyone Everywhere [Online] Available at: https://www.dignityforeveryone.org/introduction/ (Accessed: 3 March 2022).

*the concept of dignity in order to balance privacy rights and surveillance and privacy rights and legitimate state control, which has to be: a) justified, b) proportionate and c) protective for public order.*

In the three proposed characteristics offered above, we have two elements, one which control private sphere and one concerned which public control. A just society, as it will be elaborated here, will take care about both.

## 4. GDPR

'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'[21] or GDPR. The GDPR Directive entered into force on 25th of May 2018.

GDPR is an acronym derived from the first letters of the English name for the 'General Data Protection Regulation, the full title of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals concerning the processing of personal data and the free movement of such data and repealing Directive 95/46/EC'. The title itself gives us five important pieces of information: 1) 'who' passed it – the European Parliament and the Council; 2) 'when' have they passed it – on April 27, 2016; under which 'number' is it marked as Regulation of the European Union – 2016/679; 3) 'what' it deals with, i.e. 'what' is its content – the protection of individuals in connection with the processing of personal data and the free movement of such data; and 4) 'which' legal text does it replace or repeal – Directive 95/46/EC.' The next important feature to note is the very structure of the GDPR text. Viewed as a whole, it comprises two large parts: an extensive introductory part divided into 173 Recitals, and the legal text itself, which comprises 99 Articles divided into 11 chapters, of which Chapters III, IV, VI, and VII are further divided into sub-sections. Furthermore, the introductory part and the legal text itself are interconnected in such a way that each article of the legal text supports one or more of the above Recitals that explain it by giving it breadth, and describing what it aims to achieve and in what way.' [22]

21 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) is published in the Official Journal of the European Union under the code L 119, Volume 59, dated 4 May 2016. This Regulation has been also published in the Official Journal of the European Union in parallel in all European Union languages on the official EUR-Lex website [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1530652545116&uri=CELEX:32016R0679 (Accessed: 3 July 2019).

22 Same technical text has been equally written for the Savić and Mladen, 2020, p. 81.

It is obvious that, for the European Union, privacy matters. The most visible example for this is the GDPR which is connected with Art. 8(1) of the Charter of Fundamental Rights of the European Union. Although this regulation is primarily focused on the transfer of data within the European Union, it also covers transfer of data outside the EU[23]. The primary intention of the GDPR was to establish control of data usage by corporate bodies. It is intended that natural persons primarily have or gain control over their own data. As in many other big projects of law, with the passage of time, many specific problems became visible, but the massive system did not have mechanisms for easy maneuvering and treatments of special situations which were not anticipated when the GDPR was first enshrined.

Comprising 11 chapters, the GDPR became the most comprehensive and wide privacy law instrument in the EU, but according to its principles many others followed its example. The principles of the GDPR are set up in Art. 6 and show that privacy control has is limits, as shaped through the chapter on 'Lawfulness of processing'. This could be a useful guide when *balancing between public security and personal privacy and privacy of family life*. Moreover, all this should obviously be examined through the *lenses of public order and public morals*.[24]

For the aforementioned reasons, quite a few obstacles occurred in the process of implementing the GDPR principles. 1) Massive regulations are present everywhere – from internet and social media to every business activity that consumers (or those who were intended to be protected) skip reading and approve. Almost constantly, huge portions of small print are ticked automatically without any proper understanding of the contents. 2) In the beginning it was thought that the GDPR was designed only for business entities and that other entities are not covered by it, such as churches and other religious institutions. It is to be expected when one has such a

23 Art. 3(2): This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.

24 Art. 6 of the GDPR: "Processing shall be lawful only if and to the extent that at least one of the following applies:
1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." [Online] Available at: https://gdpr-text.com/hr/read/article-6/ (Accessed: 1 April 2022).

massive document that some aspects always remain uncovered and/or unpredicted. What happened was that the GDPR provisions, initially made for the protection of consumers, turned out to be obstacles which also prevented fair treatment of social entities which did not fall into a business category. This caused major controversies which were not predicted properly.

According to some relevant polls, 2 out of 5 persons are worried or concerned about the possibility that their personal data will be used without their consent or knowledge; moreover, 80% of people interviewed consider violations of financial or banking information troublesome and 62% of voters would consider the company which acquired data (which comes from their activity) directly from customers the major responsible party, and not hackers or other criminal fraudulent actors.[25] All this means that privacy issues are connected with business activity in the first place and that customers (citizens) require some serious privacy care. This also shows that the primary reason for introducing the GPDR was business activity and market logic.

Before the GDPR was introduced to the countries of the European Union, surveys were made in the United States and have shown that 72% of consumers would boycott the company which lost their private data, and that 50% would rather buy from a company that shows that it cares about the protection of private data.[26] The GDPR protects the following data:

- personal data: name and surname, address and ID number
- data printed on the credit cards
- data received through health status: sickness, invalidity etc.
- biometrics
- genetic data (DNA etc.)
- religious and philosophical convictions
- ethnicity
- economic status
- union membership
- sex orientation and sex life
- IP addresses
- Personal e-mail messages
- Cookies
- Pseudonym Data[27]

It is surely important to stress that both consent and opt-out options are present through the whole journey of processing the data of those involved. It wouldn't be wrong to say that consent and withdrawal are flip sides of the same coin. As it is well defined in Art. 7 of the GDPR:

25 Vodič kroz GDPR za početnike (GDPR Guide for Beginners) [Online] Available at: https://gdprinformer.com/hr/vodic-kroz-gdpr (Accessed: 3 April 2022).

26 Ibid.

27 Ibid. Adapted and translated to English from Croatian.

> The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.[28]

A special issue here is ensuring that children are also aware of this right in plain and clear language. Therefore Art. 12 of the GDPR clearly prescribes protection of children through appropriate language and form.[29] There is no doubt that the integral document has to be observed as a whole, but some articles underline what is the key task of the document: to give control of personal data to those who are holding and producing them: citizens. It contains: a) the right to access, which pre-includes the right to reject transfer of data and b) the right to withdraw or, said more appropriately, the right to be forgotten. Therefore it is very important to examine Arts. 15 and 17, which represent the core of the GDPR structure. The aim of this chapter is to stress and underline the pillars of the GDPR and its spirit rather than to analyze each norm of the document.

Art. 15 describes the right of citizens who have given their data to a particular entity. This is essential and a key concept in the GDPR and it comprises a) the right to access in a narrow sense, b) the right to acquire the knowledge of processing of data, c) the right to receive a copy of the data, d) the right to an explanation of how the data was used and for what purposes, e) the right to an explanation of if the data was delivered or transferred and the reasons for the same, and f) the right to know how it acquired the data, if applicable.[30] Those rights which are derived from Article 15

28 GDPR [Online] Available at: https://gdpr-text.com/hr/read/article-7/ (Accessed: 3 April 2022).

29 "The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means." [Online] Available at: https://gdpr-text.com/hr/read/article-12/ (Accessed: 3 April 2022).

30 "1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer. 3.

could be described as 1) substantive (content) and 2) processing rights. Nevertheless, it is clear that the right to be forgotten from Art. 17 is leaning on Art. 15, which states the data subject has the right to request erasure of his data as the most comprehensive and most complete right of the citizen regarding his/her private data. Even if a legitimate interest for collecting data exists, it is subordinated to fundamental rights and freedoms of the individual in case. Between approval and giving consent on one side and right to erasure are various options, variations and gradations which allow the data subject to be *in control* of his/hers personal data. Today this is done technically and automatically, which has proven to be both beneficial and hostile to the data subject. What does this means? The data subject has control over his/her data, and he/she can conduct operations connected to the transfer of personal data, which means that other companies who have legitimate interests to receive personal data can acquire those easily. However, this also includes companies which are in some sort of corporate or business cooperation to exchange data regardless of the data's ownership. This is the classical 'data portability concept'. DPC exists to prevent lockdowns of data in the business world, where it is supposedly beneficial to have data circulating for the benefit of customers, which they, at least technically, can control. Yet, massive exploitation of internet and data transmissions leads to automatic and often unfair exposure of consent documents which consumers automatically accept and forget, but the 'machine world' doesn't. This is one of the major problems of data transmission and of giving consent. One of the greatest works in this area is by law professor Frank Pasquale who described all this in his 'The black box society'[31]. As said before, between the two extremes rights, one giving (the data)

---

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. 4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others" [Online] Available at: https://gdpr-text.com/hr/read/article-12/ (Accessed: 9 April 2022).

31 Pasquale, 2016,: "Every day, corporations are connecting the dots about our personal behavior—silently scrutinizing clues left behind by our work habits and Internet use. The data compiled and portraits created are incredibly detailed, to the point of being invasive. But who connects the dots about what firms are doing with this information? The Black Box Society argues that we all need to be able to do so—and to set limits on how big data affects our lives. Hidden algorithms can make (or ruin) reputations, decide the destiny of entrepreneurs, or even devastate an entire economy. Shrouded in secrecy and complexity, decisions at major Silicon Valley and Wall Street firms were long assumed to be neutral and technical. But leaks, whistleblowers, and legal disputes have shed new light on automated judgment. Self-serving and reckless behavior is surprisingly common, and easy to hide in code protected by legal and real secrecy. Even after billions of dollars of fines have been levied, underfunded regulators may have only scratched the surface of this troubling behavior" [Online] Available at: https://www.hup.harvard.edu/catalog.php?isbn=9780674970847 (Accessed: 9 April 2022). Frank Pasquale exposes how powerful interests abuse secrecy for profit and explains ways to rein them in. Demanding transparency is only the first step. An intelligible society would assure that key decisions of its most important firms are fair, nondiscriminatory, and open to criticism. Silicon Valley and Wall Street need to accept as much accountability as they impose on others. [Online] Available at: https://www.hup.harvard.edu/catalog.php?isbn=9780674970847 (Accessed: 10 April 2022).

and one erasing (the data), there are other rights on the scale. One of those in between is the right to restriction of processing as set up through Article 18.

As said, erasure is guaranteed in Art. 17[32], but serious limitations exist and those will also be relevant when we will explain balancing between private interests and public (greater) good. As noted, this chapter is about *balancing between individual and collective (public) rights.* As stated in Paragraph 3 of the Art. 17:

> Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
> (a) for exercising the right of freedom of expression and information;
> (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
> (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3).[33]

This means that public health or public morals and interests will prevail above the interests of data subjects. This is specifically mentioned in Article 20, namely that the right to control portability will not be enforced in cases of public interests or against those rights which the controller has through official (public) rights and duties. *This is another example where balancing between different rights is taking or should take place. It is better not to use the word 'competing' rights since those different rights and interest should find their place within a coherent system of general law.*

When we examine the GDPR and its aims, it is obvious that it was tailored for the protection of the most vulnerable in the chain of business – the customer, and to give more power to the powerless – the citizen. In many cases, as it will be presented, privacy laws which were underlined and additionally enforced by the GDPR faced serious problems of classical bureaucratic influence, something that is common in legal history. Laws tend to encounter areas which were not initially meant to be tackled, and such lacunas can cause serious problems. One such problem is the application

32 "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data." Vodič kroz GDPR za početnike (GDPR Guide for Beginners) [Online] Available at: https://gdprinformer.com/hr/vodic-kroz-gdpr (Accessed: 10 April 2022).

33 Ibid.

of the GDPR on religious communities, where the same regulations are applied to churches another religious entities in the same way that they are planned for and applied to corporate bodies.

This is a complex problem. The GDPR was made for corporate bodies and legal entities which tend to be most influential in using and spreading personal data of physical persons; citizens as clients and customers. However, as it so often happens, regulations which were intended for particular entities caught in its juridical net those who were not even meant or had been planned to be involved. The GDPR has spread its scope over religious communities and sometimes this jeopardizes it fundamental functioning, which varies from State to State. In the European context, it depends on if the State has an international treaty with the Holy See and if similar agreements exist with other religious communities. It is important to stress that religious freedom(s) as have been set up in Art. 9 of the European Convention of Human Rights[34] (ECHR) protect both private and institutional freedom of religion.[35] One can't exist without the other. Particular problems arise when religious community make requests to erase or modify data which is entered in its books and registries. In brief, churches or other religious books or documents are treated as the company books of big corporations. It is obvious that this was not the intention of the lawmaker (or was it?) The consequence of strict application would have serious influence on historical books (church books are important historical materials) and could jeopardize the construction of historical facts, if necessary, and data of public interest. Such books can contain important public data.[36]

> Thus, it is clear that the European Union and its regulations accept the specificity of church/religious entities and the special way of collecting data that they perform and that are located. This does not mean at this point that they will not be affected by the GDPR, but in any case, the preconditions are created for a specific atmosphere in which churches and religious organizations will be treated.[37]

Problem of the GDPR are more delicate than one may think, as it has been demonstrated with the functioning of religious organizations and the institutional freedom of religion. Without specific practices (collecting data on baptisms, etc.) established church or religious organization cannot perform their duties and creeds

34 Art. 9 Freedom of thought, conscience and religion 1. Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance. 2. Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others. [Online] Available at: https://www.echr.coe.int/documents/convention_eng.pdf (Accessed: 13 April 2022).

35 On the issues of Church Sate Relations in Croatia and Europe see more in Savić, 2018, pp. 239–240.

36 See Savić and Škvorc, 2020, pp. 100–104.

37 Ibid. p. 8.

and therefore the GDPR jeopardize the normal functioning of religious entities. This in turn can provoke potential violations of Article 9 of the Convention. Like in many areas of privacy law, the most beneficial step to resolving the issue would be balancing.

## 5. Family as the most vulnerable – European legal framework

One of the central issues of privacy law in modern times is the Privacy of Family Life with special attention to the protection of children. Family is and should be the corner stone of European societies and deserves special protection. There are many international documents which protect family life and they are either part of the European legal structure or international covenants and treaties which overlap with the law on European ground. The most vulnerable unit in our society is its foundational unit – the family itself.

The major document of concern here is the *EU Charter on Fundamental Rights* which contains many provisions on the protection of human dignity, and guarantees legal, economic and social protection of the family and prescribes the right to private and family life, home and communications.[38] It is not pure coincidence that private and family life are in the same paragraph. Private life without protection of family life is not possible.

> Article 7 Respect for private and family life
> Everyone has the right to respect for his or her private and family life, home and communications.

In the same place, the Charter prescribes protection of personal data:

> Article 8 'Protection of personal data
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.[39]

38 Hrabar et al., 2021, p. 29.

39 Cahrter of Fundamental Rights of the European Union [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (Accessed: 29 April 2022).

On another level, the *European Convention on Human Rights* states that everyone has the right to protection of private and family life, and here, again the treaty combines and puts into connection those two terms – private life and family. As a matter of fact, the EU Charter and ECHR have minor differences in their respective texts, but Art. 7 of the EU Charter and Art. 8 of ECHR are twins.

> Article 8 'Right to respect for private and family life
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[40]

As Hrabar explains succinctly, the judicature of the European Court of Human Rights shows that many family law cases are connected with numerous questions which have to be addressed by local courts and other state bodies in order not to have human rights violations.[41] Furthermore, ECHR contains a precise catalogue of human rights and discrimination violations on various grounds and therefore legal theory should find a way to apply the Convention as a 'living instrument' which has to be used in accordance with specific circumstances of the case.[42] Although generally correct, this statement also contains possible traps because it allows interpretations that allow permanent change, which could put into jeopardy public morals. There are some foundational principles which are permanent and universal and unchangeable in its essence and are not prone to interpretations. This is connected with theories of natural law.[43]

Moreover, it is important to stress that the European Court applies the British doctrine of Margin of Appreciation, which allows the court to somehow treat differently similar cases from different countries. It means that the court will take into account various sociological, historical and ontological perspectives when discussing cases from various countries. This will allow it to preserve values of particular countries. It will be found that cases from Central and Southeastern Europe bear different substance than for instance those from the North or partially from the West of Europe: family law is deeply rooted in values and traditions of particular countries, but this should exclude new movements and different opinions. Again, the key is balancing.

40 European Convention on Human Rights (ECHR), Art. 8 [Online] Available at: https://www.echr.coe.int/documents/convention_eng.pdf (Accessed: 29 April 2022).
41 Hrabar et al., 2021, p. 12.
42 Ibid. p. 13; According to: Hugh, 2010, p. 78.
43 Savić, 2021, p. 18. Also see Hrabar and Dubravka, 2018, p. 52.

At this juncture, it is important to stress that privacy law in family life is also implanted into the domestic internal law of particular member states of the ECHR. For instance, Croatian Criminal Law, through the Croatian Criminal Code, specially protects privacy of the child and prescribes prison penalties up to two years.[44] This is the case with many other jurisdictions.

## 6. Doctrinal approach to the issues of privacy in family law

There are numerous debates about the extent of state intervention into the private life of families, especially in relation with the right of parents to educate their children according to their philosophical and religious convictions. There are various aspects of privacy law interfering with family life: a) the right of the parents to educate and raise their children, b) the right of the family to be protected from outside influences, c) the obligation of parents to take the best care possible of their children's needs and interests, d) the obligation of the State to provide a proper and decent legal, and then social, framework for family life, e) the obligation of the State to supervise the educational system for the best interests of children and f) the obligation of the State to intervene into the life of families in case of violence, crime, and especially if children need special protection.

As we can see from the list of interactions between state, family and privacy, most components show that family is a private affair, wherein rights of the family itself and of parents in particular with regard to their children outnumber the rights of the State towards the family. State rights are in their nature obligations, often concerned with child protection. The state has an obligation to interfere when crime or violence is involved and when children need protection.

According to Neethling,

> privacy is personal living condition which is characterized by the person's right to decide by himself/herself or to control the scope of her privacy which can be

44 Art. 178 Croatian Criminal Code [Online] Available at: https://zakonipropisi.com/hr/zakon/kazneni-zakon/178-clanak-povreda-privatnosti-djeteta (Accessed: 30 April 2022).
"(1)Tko iznese ili pronese nešto iz osobnog ili obiteljskog života djeteta, protivno propisima objavi djetetovu fotografiju ili otkrije identitet djeteta, što je kod djeteta izazvalo uznemirenost, porugu vršnjaka ili drugih osoba ili je na drugi način ugrozilo dobrobit djeteta,
kaznit će se kaznom zatvora do jedne godine.
(2)Tko djelo iz stavka 1. ovoga članka počini putem tiska, radija, televizije, računalnog sustava ili mreže, na javnom skupu ili na drugi način zbog čega je ono postalo pristupačno većem broju osoba,
kaznit će se kaznom zatvora do dvije godine.
(3)Tko djelo iz stavka 1. i 2. ovoga članka počini kao službena osoba ili u obavljanju profesionalne djelatnosti,
kaznit će se kaznom zatvora do tri godine."

intruded by the breaking into the personal sphere of individual or by disclosing or publishing private facts.[45]

There are more and more scholars of civil law who have started to recognize that a large amount of civil law protections falls within the scope of the protection of the right of personality. It is interesting that both continents espousing so-called Western thought, North America and Europe, had similar developments in terms of regulating personal rights. For instance, rights which protect private life; first economic rights were developed and regulated, and only after existential issues were settled, states both on the American continent as well as States in Europe came to build the legal framework for the protection of personal rights.[46]

Radolović is absolutely right when he states that the development of personal rights was less 'visible' than property or financial rights; it is a product of the development of the human race and the development of law in general.[47] It is interesting that none of the totalitarian regimes recognize personal rights[48] from which privacy law is also derived. This is somehow obvious – totalitarian regimes do not accept free will of the person and State intervention is more a norm and less of an exception. This was the case with the totalitarian regimes of Nazism, Fascism and Communism, which had swamped European lands for decades. Authoritarian regimes do not respect individual freedoms. Since freedom for the family's privacy can only be derived from individual freedom, in those systems neither existed. The veil of collective security, or to put it as a more sharpened expression, collective surveillance, which is always in the hands of the group(s) who dictate, is just another expression for suppression. On the other hand, democratic regimes are based on the principle of personal rights, which is the basis for the protection of privacy law and the privacy of families in particular.

*Table 1*

| **REGIME** | **MAJOR VALUE** | **MAJOR ACTION (ACTIVITY)** |
|---|---|---|
| Totalitarian regime | Collective Security | Control |
| Democratic regime | Individual Liberty | Privacy |
| Balanced regime (democratic) | Public order | Protection |

45 Neethling, 2005, p. 210.

46 Radolović, 2006, p. 1. This is interesting analysis of professor Radolović, who explains that the first values which were protected were those of material and financial substance, connected to property like money, capitals, real estate, interests, security issues etc. It seems, however, that now there is some shift happening and that more and more space is dedicated to personal rights and their connection to property rights within the one general system of civil law. Security and safety of private life enter more into focus and discussion of the security of the State activates only if private life threatens society or its principal values and if the *veil of private life* protection hides unwanted behavior towards children, p. 130.

47 Radolović, 2006, p. 131.

48 Ibid.

Table 1 shows three possible systems which have existed both historically and/or presently. Totalitarian regimes claim collective security, but this is usually only an excuse for a control mechanism. In this system, collective security is a justification for law-making in order to gain control. In democratic regimes, the main social value is individual liberty and the law which covers it is shaped to secure privacy as a goal. And the third regime shows a balance between extreme requests of collective security and absolute individual liberty, in a system where public order is a value protected by law and where the main goal is to secure the real protection of both private and family life, but secure the protection of the values of a particular culture and public order as well. Having that in mind alongside the judicature of the European Court of Human Rights, we can claim with great certainty that the level of protection would fall under the application of the Margin of Appreciation doctrine through which the Strasbourg court takes into account particularities of each country as quaestio casii with potentially different solutions. It does not mean that a balanced regime is not democratic; on the contrary, balanced regimes are democratic and safe for everyone – they comprise both security and individual liberty as values that have to be protected in order to maintain public order. They contain the modification of the totalitarian regime's most prominent characteristic, security, and the democratic regime's most prominent characteristic, individual liberty. Just to avoid confusion, there might be traces of protection of individual liberty in totalitarian regimes and even some elements of individual liberty practices, but that regime is unacceptable because it is focused only on the needs of the collective body (State), usually meaning political elites with doubtful legitimacy and/or legality. Democratic regimes have various gradations for the protection of public order and public morals, but usually they focus on personal rights rather than the norms of society (or norms and values of society are only transmitted to the values of individuals). Balanced regime protects both, but as said, elements of a balanced regime could exist in other legal (State) systems.

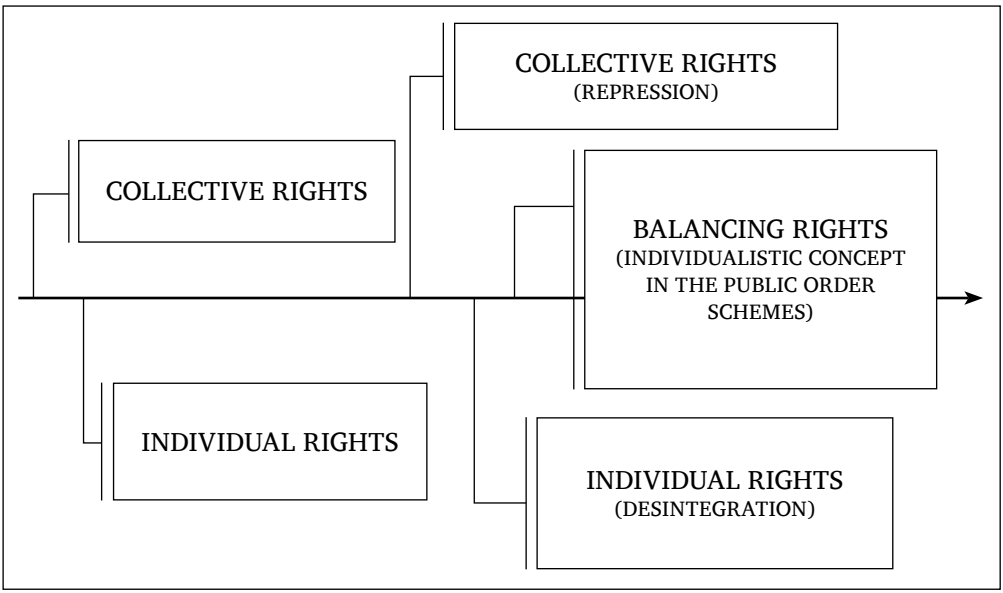
In a particular sense, personal rights are also part of the person's property but those properties are not *stricto sensu* materialized.[49] Radolović succinctly states that the major difference between personal rights and property rights is that personal rights are bound with the verb 'to be', and property rights with the verb 'to have'; different verbs and different primary positions. Then again, only those personal rights which could be transferred into property rights in the term that can be materialized will be objects of private law.[50] In that sense, violation of privacy of particular person in respect of publishing his/hers personal details (and his/hers family life details) will be the subject of private law and thus grounds for legal action.[51]

In his quoted article, Radolović makes necessary connections between religion and personality rights which are linked to the development of privacy law. In the construction of privacy law and the right to privacy, references to religion and religious laws are

49 See Ibid. pp. 133 et seq.
50 Radolović, 2006, p. 134. In his footnote 4., according to: Perlingieri, 1972, p. 15.
51 Ibid. pp. 135; 140.

inevitable.[52] Such statements are connected with discussions on human dignity, which were elaborated in the Declaration on Human Dignity for Everyone Everywhere signed in December 2018 in Punta del Este in Uruguay. With the development of the human race, personality rights were more or less developed, but specially so in the period of humanism and Renaissance and later in the age of the so called 'era of the great ideas', wherein numerous codifications took place on the European continent.[53] It is right to claim that the 20th century was a step backward to begin with, in the context of personal rights of citizens[54] – totalitarian regimes brought forth numerous movements that supressed the private sphere. In the history of the development of individual rights, there were slopes in which collectivity had a primary influence on societal norms, while modernity brought with it more individualistic concepts of social behaviour. Such shifts have changed again and it is clear that a purely individualistic approach to human behaviour lacks the ability to build collective cohesion in society, which is built on particular norms and values. One is sure that historically we face permanent changes of those two distant concepts.[55] Collective rights throughout history, as written here and in many other places, are the key for today's democratic societies, which should practice balancing, or as Aristotle would say, seek for *mesotes*, or the 'golden middle' between collective rights which are bound to today's public order schemes and individual rights which are connected to dignity claims and subsequently privacy rights.

*Figure 1 Timeline of the historical movement of collective and individual rights*




52 Ibid. pp. 136–137.
53 Radolović, 2006, p. 137.
54 Ibid.
55 Savić, 2013, pp. 1–11.

## 7. On natural law, privacy and family

Family is the core of society. It remains as such even now. Therefore it requires special protection. Despite the fact that the notions on family and family life change from those on the liberal end of the spectrum, in the Central and Eastern Europe particularly, where classical concepts of family exist, family ties are still strong (e.g. children live close to parents; many generations live together, children visit parents and relatives often, (grand) parents help their children with their children etc.).

This is contained in the teachings of natural law jurisprudence, which posits the values of family life as values which arise from divine law (examples of family life from the New and Old Testament, but also at other primary canonical sources of other religions, and/or natural order of things). As Radolović stated, the school of natural law have made an important impact on the law of personality as well as privacy law by pointing at the important gap which cannot be described by positive laws and is rooted in dignity and claims that each person has their essential rights as shaped by human rights law.[56] Therefore and in accordance with natural law, all personal laws as well as privacy law should be protected for its values which are in the first place of non-materialistic fibre. That violation of privacy law, in the legal action, ends up resulting in something which is at the end very materialistic, that is money paid for as compensation or by the publishing of a statement as a way of restitution, is obvious. However, this, even more than anything, shows that natural law has its core influence in the foundations of privacy law.

There are opinions that claim that privacy law also expands to artificial legal bodies and legal entities such as corporations[57]. The prevailing opinion is (and should be) that those who bear the legal personality and ability to request protection for their privacy are physical (natural) persons. Individual physical persons should be treated as the bearers of privacy law. Although initially natural law theories argued that personal rights are linked to elitist concepts of the protection of people with special qualities, the prevailing attitude is still that those rights have to be recognized on the grounds of human dignity, and talents should be considered as natural or divine implants into humans creature which than have to be used in the proper way of serving the community. For such reasons and on those grounds, natural persons deserve to be protected.

Individual private life is protected: a greatest product of individual private life is family as a unity of two people who create their own private space. The greatest and the most important issue here is the right of the child to have their privacy, and to be protected in totality of their being. Children as well as people with disabilities have a right to privacy. This has to be examined through the lens of family law which prescribes that parents or other legal guardians have the explicit right to represent children and protect their privacy, including their capacity to restrict or expand the

56 Radolović, 2006, p. 139. See also: Declaration on human dignity for everyone everywhere. See supra.
57 See in Radolović, 2006, p. 14; and then Gavella and Klarić, 2000, pp. 1–63; p. 34; Klarić, 1998, p. 95.

child's privacy with respect to the public use of their image and/or work. A typical example for this arises when parents are required to sign permission for the usage of the child's face in filmed material (such as in kindergarten for a show which they have been performing). In the modern era this is most visible in situations where parents post tons of photographs of their children on social media, violating their privacy out in public space. This only shows that family holds, or is entitled, to a specific treatment when we discuss privacy; particularly, not the family itself, but the parents. Sometimes the consequences of this right are not what we might desire, as it is mentioned in the latter example with social networks. The real proof that family and parents in particular have the right to privacy and to control the privacy of their children is an institutional representation which is very explicit and gives to parent tremendous acknowledgment for performing their parental duties.[58]

In this respect, we have to acknowledge that privacy law encompasses all members of the family and that principal bearers of the right to privacy are parents who decide on behalf of children. Of course, it is more than clear that children have their own rights which have to be acknowledged and respected but, at this juncture, we will discuss the right of parents to educate their children in accordance with their moral and philosophical convictions, and that they should not be distracted from this role since children primarily belong to parents and to the State.

As it was elaborated in preceding paragraphs, the State has the right and duty to control and intervene in special and unusual circumstances. Family life connected with moral and philosophical convictions and attitudes which include various world-views followed by parents and subsequently by their children is a private affair of every family as an organizational unit of society. Of course, it might so happen that private life and life of a society as a whole produces different paths, but in those cases, balancing, which has been mentioned several times, plays a crucial role. The famous case of *Lautsi v. Italy*, is the perfect example to show how the philosophical convictions of parents came into some sort of clash with specific values which exist in society, and legal actions were needed to settle the issue.[59] In this landmark case,

58 Savić, 2021, p. 82; Hrabar et al., 2021, pp. 175 et seq.

59 Lautsi v. Italy, ECHR case [Online] Available at: https://adfinternational.org/lautsi-and-others-v-italy/ (Accessed: 21 September 2022). Also see Savić, 2020, pp. 11–37. The Lautsi family was an agnostic family from the Veneto region of Italy. Their claim was that the crucifix in the classroom presents a threat to the principle of the separation of Church and State guaranteed by the Italian Constitution. All Italian classrooms in public schools have crucifixes attached to a wall, all of them from Trieste to Sicily. Italian courts rejected the claim, but the first instance court of the European Court of Human Rights decided that the Lautsi family has the right and that the Italian state violated Art. 9 of the European Convention on Human Rights which guarantees freedom of religion (but also as J. H. Weiler nicely elaborated, 'freedom from religion'). The Grand Chamber of the Court decided that the crucifix in the classroom does not harm anybody but is a mere expression of Italian tradition and identity and that the claim of Lautsi family was not justified according to the Convention. The European Court of Human Rights uses (and it did so in this case) the Margin of Appreciation, an old British doctrine which allows the Court and judges to take into account all relevant elements and data which are existing in a particular state and its society, such as moral, religious, traditional, and geo-political elements, among others.

everything came to one table – the right of parents to educate children according to their moral and philosophical convictions was examined in conjunction with other values which exist in the Italian state. The Lautsi family has the right to educate their child in a specific worldview framework of their family. They have the right to live an agnostic life despite the fact that they live in Italy which is predominantly Catholic and where Christianity is obviously deeply rooted in its culture. Moreover, what we have here is a clear example of the secular State which uses the cooperation model, allowing the exercise of various interactions between Church and State for historical, traditional, and humanitarian reasons, among others.[60] We also see the exact consequence of balancing – family is entitled to have their own private life, but this has to be in accordance with the ultimate moral values of the state itself. It is not always easy to find that balance. As a matter of fact, sometimes it is quite hard.

When we discuss the broader spectrum of application of personal laws and privacy in particular, we can see that civil law, which was traditionally connected to property law, shifts from that to a position with more delicate personal law protection. This represents a significant change in the treatment of privacy law and personal laws in general. Material substance is not any more a prevailing element of civil law, but rather only one part of it.[61] In the development of civil law in the EU (Civil Code of the European Union)[62], it was noted that traditionalist views on the nature of civil law caused delays in the acceptance of personal law within the broader meaning of civil law in general.[63] The development of the right of personality and its struggle to become a part of civil law follows several general trends and the development of complete law in general. Social and economic development opened humanistic approaches to law, and civil law was not the exception by any means. The special (avant garde) quality of humans are our 'bio – cultural value' which receive special form with legal protection.[64] The substance of this phenomena is the internal value of a human's existence, their characteristics, views, appearance and ways how they handle and produce things, their thoughts and secrets, opinions and aspirations, and all those values they consider important. This is the real background of the right to privacy and the basis for privacy law. Radolović is right when he says that this process is in the making; he states that normative regulation does not resolve everything and much depends on socio – legal conditions which are necessary for liberal democracy and cultures of respect (respect of human beings and their values)[65]. Here it is important to stress that respect for human beings and their values should be based on the concept of dignity, which has to be protected. Human dignity is, as it was mentioned before, a source of human rights and the source of basic needs of every human being to be protected in their internal values

60 See Norman, 2013, p. 14.
61 Radolović, 2006, p. 130.
62 See more in Collins, 2008.
63 Ibid.
64 Collins, 2008, p. 131.
65 Radolović, 2006, p. 131.

and manifestations of will, which is the most sacred part of man, received by God or Nature and as such should be protected by law. Man cannot really be free if their values and their family lives are not protected by law. Without protection, privacy law doesn't make sense, and only with legal protection of values, society gives what is necessary for dignitary actions.

Having said all that, the only logical conclusion is that the privacy law of a person who has the rights for self and for others (children) is protected by contemporary laws of the newest generation in this stage of human development, which is coming back to the core of legal protection – a human person in their totality. The scope of the rights of families to educate children in accordance with their moral, philosophical and religious beliefs is the cornerstone of the right of parents to guide the child *in* and *for* life. As Hrabar elaborates, education and upbringing (which includes moral lessons) are equally important and the totality of those rights belong to parents[66]. Therefore, discussions which may be dissonant and differently shaped and which precede parents' discussions on various questions are private affairs of the family and as such are protected by law. It is interesting to note that various legal systems define this through different wordings, but with the same meaning: it seems that development of law resulted, at least in this area, in the understanding that protection of integrity – which includes privacy – of family life means a just and balanced society in which *State and parents are partners*. Parents are trusted that children will be taken care of and the State intervenes only when it is necessary. Parents enjoy freedom in their private decisions, sometimes with social implications. Great examples are the Irish and German Constitutions mentioned in Hrabar's work. [67] At the same time, the German constitution describes the right to upbring and educate children as parents' *natural right.*[68] Similar solutions exists in the Croatian constitution.[69]

66 Hrabar, 2018, pp. 321–322.

67 Ibid. p. 324, see footnote 17. Irish Constitution: Art. 42.: "1) The State acknowledges that the primary and natural educator of the child is the family and guarantees to respect the inalienable right and duty of parents to provide, according to their means, for the religious and moral, intellectual, physical and social education of their children."

68 Ibid. see footnote 18. „Pflege und Erziehung der Kinder sind das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht. Über ihre Betätigung wacht die staatliche Gemeinschaft.", a autorica prema [Online] Available at: https://www.bundestag.de/parlament/aufgaben/rechtsgrundlagen/grundgesetz/gg_01/245122 (Accessed: 21 September 2022).

69 Constitution of the Republic of Croatia (Ustav Republike Hrvatske), National gazette of the Republic of Croatia (Narodne novine), br. 56/90, 135/97, 113/00, 28/01, 76/10, 5/14.; Art. 63 'Parents shall bear responsibility for the upbringing, support and education of their children, and they shall have the right and freedom to make independent decisions concerning the upbringing of their children. Parents shall be responsible for ensuring the right of their children to the full and harmonious development of their personalities. Children with physical and mental disabilities and socially neglected children shall be entitled to special care, education and welfare. Children shall be obliged to take care of their elderly and infirm parents. The state shall devote special care to orphans and minors neglected by their parents.' Full and consolidated text of the Croatian Constitution in English is [Online] Available at: https://www.usud.hr/sites/default/files/dokumenti/The_consolidated_text_of_the_Constitution_of_the_Republic_of_Croatia_as_of_15_January_2014.pdf (Accessed: 24 May 2022).

The right to education is defined in Article 2 of the 1st Protocol of the European Convention of Human Rights:

> No person shall be denied the right to education. In the exercise of any functions which it assumes in relation to education and to teaching, the State shall respect the right of parents to ensure such education and teaching in conformity with their own religious and philosophical convictions.[70]

This is directly connected with the right of parents to educate children in their own view and according to their principles of conscience. Thus it is well elaborated in the Guide on Art. 2 of Protocol, No. 1 to the European Convention on Human Rights – Right to Education, wherein several articles are connected with those specific parent's rights through Arts. 8, 9, 10 and 14 of the ECHR. The wording of the First Protocol is connected with Art. 9 (conscience and religious freedom) through cases *Folgerø and Others v. Norway*; *Lautsi and Others v. Italy*; *Osmanoğlu and Kocabaş v. Switzerland*; Art. 8 (privacy) through cases like *Catan and Others v. the Republic of Moldova and Russia;* and Art. 10 (free expression) through case like *Kjeldsen, Busk Madsen and Pedersen v. Denmark*.[71] At the same time, the European Court is clear that parents cannot deny children's right to education *(Konrad and Others v Germany)* and that the child cannot sue parents on the grounds that they have performed rights guaranteed by Convention and Protocols *(Eriksson v. Sweden)*. This is the perfect example of how *rights have to be balanced in order to protect public order and public morals*. Yes, parents have the right to privacy of family life, but there are 'public limits' to those.

## 8. Conclusion: Balancing

It seems that the perception of the contemporary world is one comprising individuals with numerous identities which are protected by law. Human identity has many faces, some of them external (visible) and some of them internal (not visible; hidden). Both hidden and visible identities, in a world governed by the rule of law and human rights, are protected by personality rights and privacy law, which became the most delicate and profound manifestation of modern civil law. We also live in a world of controversies and often between highly antagonized positions which have been dug into deep corridors without real and honest communication. In such a world, *law has a crucial role in shaping and balancing different worldviews that exist in the public sphere*. This is the personal dimension of law: to secure different and often

70 Hrabar, 2018, p. 330.
71 Ibid.

polarized stands and attitudes and ensure they can live harmoniously in one society. There is another dimension of law which arises from the obligation of the state to protect public values of the state which are not of conflicting nature. What does this mean? It means that the body of law comprises many values which are spread around various branches of law and legal institutions. As law is (or at least should be) a coherent body, it has to be presumed that different norms and solutions have to be in accordance with each other, but even more importantly it is necessary that law looks like coherent body which has parts which work on the same frequency.

Historically, there were numerous shifts between collective and individual rights, from the rights of tribes and nations to the rights of groups and finally individuals. Changes in the society, and therefore in law, are usually circular, and our civilization departed from collective right to the rights of individuals and back. Aristotle's views on *mesotes* usually give a solution which is inclusive and seeks to accommodate values the both ends of the spectrum; that those values have to belong to the same coherent system of law. It means that we need a system which will take into account both realities: *individual freedoms and private space, but also obligation of the state to protect public order and the most vulnerable*. After examining many aspects of privacy law, especially doctrines which can be found in the European context, it becomes clear that protection of family law and privacy of family life has it all, and it is a real amalgam of an example of protecting both – privacy of parents and their rights to educate children in accordance with their philosophical, moral and religious beliefs which includes, but it is not limited to religious education, church attendance, praying etc. on one side; and protection of children on the other. Parents do have the right to educate children, but they have to obey the general educational framework of the state and therefore should follow at least the minimal requirements of the society in which they live. As always elaborated, the relationship between physical persons and the State should always be made in the form of *dialogue*. This means that relationships between individuals and the State, which are so evident and visible in privacy law, are *two way streets*. On one hand there are high and excepted standards of personal status and private life, but on the other hand there are requests of security and protection of the most vulnerable. Obviously the key is *balancing*. Only a society which is taking care of the *needs of its individual citizens on the one side and social cohesion on the other can really be democratic and prosperous.* Hence, there is no prosperity for the nation where there is no prosperity for the individual. In line with that, there is no security of the individual where there is no security of the nation.

# Bibliography


Brayne, H., Carr, H. (2010) *Law for Social Workers*. Oxford: Oxford University Press.

Collins, H. (2008) *The European Civil Code: The Way Forward*. Cambridge: Cambridge Studies in European Law and Policy, Cambridge University Press; https://doi.org/10.1017/CBO9780511620010.

Diggelmann, O., Cleis, M.N. (2014) 'How the Right to Privacy Became a Human Right', *Human Rights Law Review*, 14(3), pp. 441–458 [Online]. Available at: https://doi.org/10.1093/hrlr/ngu014 (Accessed: 04 November 2022).

Doe, N. (2011) *Law and Religion in Europe: A comparative introduction*. Oxford: Oxford University Press; https://doi.org/10.1093/acprof:oso/9780199604005.001.0001.

Gavella, N. (ed.) (2000) *Osobna prava – I. dio*. Zagreb: Pravni fakultet Sveučilišta u Zagrebu.

Griffin, J. (2007) 'The Human Right to Privacy', *San Diego Law Review*, 44(1), pp. 697–719.

Hrabar, D. (2018) 'Odjek roditeljskih vjerskih i filozofskih uvjerenja na odgoj i obrazovanje djece u hrvatskoj legislativi', *Zbornik Pravnog fakulteta u Zagrebu*, 68(3-4), pp. 319–336 [Online]. Available at: https://hrcak.srce.hr/207486 (Accessed: 04 November 2022).

Hrabar, D., Hlača, N., Jakovac-Lozić, D., Korać Graovac, A., Majstorović, I., Čulo Margaletić, A., Šimović, I. (eds.) (2021) *Obiteljko parvo*. Zagreb: Narodne Novine; https://doi.org/10.3935/zpfz.71.5.08.

Klarić, P. (1998) 'Odgovornost za nematerijalnu štetu pravnih osoba u gospodarstvu, Zbornik radova XXXVI. susret pravnika u gospodarstvu', *Zbornik Pravnog fakulteta u Zagrebu*, 95(4), pp. 522–538.

Neethling, J. (2005) 'Personality rights: a comparative overview', *Comparative and International Law Journal of Southern Africa*, 38(2), pp. 210–245.

Pasquale, F. (2016) *The Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press; https://doi.org/10.4159/harvard.9780674736061.

Perlingieri, P. (1972) *La personalità umana nell´ordinamentno giuridico*, Università degli studi di Camerino: Jovene.

Radolović, A. (2006) 'Pravo osobnosti u novom Zakonu o obveznim odnosima', *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 27(1), pp. 129–170.

Radolović, A. (2006) 'Pravo osobnosti u novom zakonu o obveznim odnosima', *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 27(1), pp. 129–170 [Online]. Available at: https://hrcak.srce.hr/clanak/12466 (Accessed: 04 November 2022).

Savić, V.-I. (2013) *Razumjeti kaznenu odgovornost pravnih osoba*. Zagreb: Pravni fakultet u Sveučilišta Zagrebu.

Savić, V.-I. (2019) 'Charles Habib Malik and Reflections of a Lebanese Multi-Religious Landscape. A Comment Written on the Occasion of the Celebration of the 70th Anniversary of the Universal Declaration of Human Rights', *Zagrebačka pravna revija*, 8(2), pp. 175–176 [Online]. Available at: https://hrcak.srce.hr/240722 (Accessed: 04 November 2022).

Savić, V.-I. (2019) 'State and Church in Croatia' in Robbers, G. (ed.) *State and Church in the European Union*. 3rd edn. Baden-Baden: Nomos, pp. 239–240; https://doi.org/10.5771/9783845296265-239.

Savić, V.-I. (2020) 'The legal regulation of religious symbols in the public sphere in Croatia', in Sobczyk, P. (ed.) *Religious Symbols in the Public Sphere, Analysis on Certain European Countries*. Budapest: Ferenc Mádl Institute of Comparative Law, CEA Publishing, pp. 11–38; https://doi.org/10.54237/profnet.2021.psrs_1.

Savić, V.-I. (2021*) Bilježnica za razumijevanje prava i države*. Zagreb: Naklada Slap.

Savić, V.–I., Škvorc, M. (2020) 'Keeper of Tradition and Divine Law in the times of identity crisis: Catholic Church and demands of GDPR in the Eu and Croatia', *Revista Forum Canonicum*, 15(1), pp. 77–104.

Savić, V.–I. (2016) 'Still Fighting God in the Public Arena: Does Europe Pursue the Separation of Religion and State Too Devoutly or Is It Saying It Does Without Really Meaning It?', *BYU Law Review*, 45(3), pp. 679–726 [Online]. Available at: https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=2984&context=lawreview (Accessed: 04 November 2022).

Solove, D.J. (2022) 'Conceptualizing Privacy', *California Law Review*, 90(4), pp. 1087–1155 [Online]. Available at: https://doi.org/10.2307/3481326 (Accessed: 04 November 2022).

Warren, S.D., Brandeis, L.D. (1890) 'The Right to Privacy', *Harvard Law Review*, 4(5), 193–220 [Online]. Available at: https://doi.org/10.2307/1321160 (Accessed: 04 November 2022).

Chapter III

# The Protection of Privacy in the Hungarian Legal System, with Special Regard to the Freedom of Expression

András Koltay

## 1. Introduction

The protection of privacy represents a major challenge for legal systems, especially in light of the proliferation of new technologies for monitoring and recording individuals, with a public increasingly hungry for news and confidential information. The balance between the protection of privacy and the rights and interests of the public (freedom of speech, freedom of the press, being informed on public issues, freedom of information) is difficult to strike and necessarily remains fragile. This chapter examines the Hungarian legal system, both in terms of regulation and practice, primarily from the point of view of how to define the balance between privacy and the right to freedom of expression. After offering a general overview in Section 2, the provisions of the Fundamental Law are examined in Section 3, followed by a discussion of the issues arising in private law in Section 4, while Section 5 provides an overview of the protection of privacy in criminal law. The paper then goes on to cover data protection (Section 6) and administrative procedures (Section 7) before attempting to draw general conclusions (Section 8).

András Koltay (2023) The Protection of Privacy in the Hungarian Legal System, with Special Regard to the Freedom of Expression. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 77–109. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_3

## 2. General overview

Privacy, according to Robert Post, is one of the social norms that ensure the existence of the individual and the survival of the community, which is made up of autonomous individuals.[1] Fortunately, one might say, the instruments available to the law are incapable of providing a satisfactory answer to all the questions that arise in the context of private life. In the modern era, the value of the protection of privacy gradually gained recognition. In the early nineteenth century, Benjamin Constant disapprovingly claimed in his 1819 essay, "The Liberty of Ancients Compared with that of Moderns," that the private sphere of modern human beings was better protected than it had been previously, but that in the meantime he is deprived of the possibility of participating in making decisions on the affairs of the community.[2]

Privacy is usually understood in different legal systems to include various partial rights, themselves sometimes named and sometimes unnamed in statutes. The US view of privacy also considers certain elements of the right to self-determination to be relevant to privacy, such as the right to control one's own body (and deriving from this, for example, the right to abortion),[3] while the case law of the ECtHR applies Art. 8 of the European Convention on Human Rights in a general civil liberty sense. In the following analysis, I shall limit the discussion to problems related to potential clashes between the private sphere and the rights to freedom of speech and freedom of the press.

As Elemér P. Balás, the first Hungarian theoretician of personality rights, put it, the law "respects the right to disgust from the public."[4] The starting point in the legal history of this issue is Samuel Warren and Louis Brandeis's classic study *The Right to Privacy* published in the *Harvard Law Review* in 1890, which explicitly stated the need for "the right to be left alone" in the face of the tabloid press, which was already a growing problem in their day.[5] According to the authors of the article, the insatiable appetite of the press for new sensations and "rumours", and the development of photographic techniques was endangering, to an unprecedented degree, the sovereign, inner world of the individual and its inviolability.

The approach of treating privacy as a value somehow related to the protection of human dignity is characteristic of continental Europe, while that of treating privacy as an aspect of the protection of personal freedom (freedom of choice) is characteristic of Anglo-Saxon legal systems, although this does not necessarily lead to practical differences in the assessment of certain facts. Even in European legal systems, the violation of human dignity is not a necessary condition for establishing an infringement as it may, for example, be infringed in cases relating to personal data,

1 Post, 1989.
2 Constant, 2016.
3 Rubenfeld, 1989.
4 Balás, 1941, pp. 653–654.
5 Warren and Brandeis, 1890.

private dwellings, the right to one's own image or likeness and the protection of private communications without violation of human dignity occurring. The right protects the person's freedom of choice and, if the freedom of choice reserved for him or her is infringed by the intervention of others, the infringement will be deemed to have occurred, even if the infringement does not otherwise undermine their dignity. Thus, if someone is photographed in their private dwelling, their right to privacy is violated, even if the image is not otherwise capable of violating their human dignity.

The current state of the information society poses greater threats to privacy than ever before, due to the technological advances that shaped it. The best-known literary depiction of the violation of privacy—and of the way it leads to the dehumanization of society—is undoubtedly George Orwell's *Nineteen Eighty-Four*.[6] Banned for decades in the eastern part of a divided Europe, the book is now read as a universal warning, not just as an indictment of totalitarian dictatorships. At the same time, the state's role as Big Brother has been joined by a number of "Little Brothers," concentrations of power which, despite having different interests, have also become enemies of privacy. They typically accumulate data on citizens for business purposes, to categorize them and find out about their shopping habits and even which books they read.[7]

The freedom of speech is, of course, protected to a certain extent, even if its exercise involves indulging in private pursuits, disclosing secrets, or taking pictures without consent. Concerning matters of public interest, the extent of the protection of privacy is more limited. Moreover, libelous statements are more tolerated if they are made in relation to matters of public interest. However, the category of matters of public interest should be construed in a limited sense: Not all matters in which the public may be "interested" are regarded as matters of "public interest."[8] This principle is reinforced by the ECtHR in its landmark decision in *Von Hannover v. Germany*:[9]

> The Court considers that a fundamental distinction needs to be made between reporting facts—even controversial ones—capable of contributing to a debate in a democratic society relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who, moreover, as in this case, does not exercise official functions. While in the former case the press exercises its vital role of "watchdog" in a democracy by contributing to "impart[ing] information and ideas on matters of public interest"…it does not do so in the latter case.[10]…As in other similar cases it has examined, the Court considers that the publication of the photos and articles in question, of which the sole purpose was to satisfy

6 Orwell, 1949.
7 Majtényi, 2006, p. 47.
8 See *Campbell v. MGN* [2004] 2 AC 457, HL.
9 Application no. 59320/00, judgment of 24 June 2004.
10 Ibid. para. 63.

> the curiosity of a particular readership regarding the details of the applicant's private life, cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public.[11]

The privacy of politicians and of the representatives of state power is also protected, just as that of ordinary citizens. However, which events or pieces of information relate to carrying out the public function of such persons, and therefore may be disclosed to the public is—and indeed, should be—open for debate. The extended scope of the freedom of the press as it applies to celebrities and the infringement of the privacy of celebrities is also subject to discussion. Similarly to persons exercising state powers, the starting point here is that even the most exposed celebrities have a certain private sphere that should be protected, the infringement of which is not justified by any public interest consideration. However, and unlike for persons exercising real powers, instances of matters falling within the privacy of celebrities that are relevant for deciding on public matters seldom arise. Liability for infringements of the privacy of celebrities is shared, at least between the press and the celebrity trying to protect their privacy. On the one hand, celebrities seek publicity, thrive on it, and ultimately make their fortune by appearing publicly. On the other hand, "stars" enjoy publicity only as long as they can benefit from it; a time may come when celebrities wish to withdraw to their autonomous private sphere.

The various aspects of protecting privacy against the freedom of speech and the freedom of the press may be hard to fit into clear-cut and well-defined legal categories, such as libel or defamation. One may consider the right to privacy to be the equivalent of a general personality right, or the general clause of personality rights.[12] It would be hard to draw up any exhaustive list of the various facts that can be relied upon to define an abstract set of circumstances covering all possible cases where there are conflicts between the freedom of speech and the right to privacy. According to William Prosser's categorization, which has come to be regarded as a classic, the different types of the privacy tort are as follows:

- invasion of privacy—the activity of obtaining confidential information;
- publishing embarrassing, private (true) information;
- misrepresenting a person by publishing facts that are true or even false but not defamatory;
- unauthorized use of a person's name or image for commercial purposes.[13]

To this can be added another type, covering cases of unauthorized disclosure of identity for which, while they might be included in the "publication of embarrassing information" above, separate treatment is justified, mainly because of the different nature of applicable regulations.

11 Ibid. para. 65.
12 Sólyom, 1984, p. 667.
13 Prosser, 1960.

## 3. The Fundamental Law of Hungary

Art. VI of the Fundamental Law of Hungary, in force since 2012, protects the right to the inviolability of private life, the content of which has been significantly expanded by the currently effective Fundamental Law, compared to the rules of the previous Constitution (effective prior to 2012). The Fundamental Law protects private and family life, and accords a constitutional level of protection for the home and for communications and data of public interest. The Fundamental Law requires the establishment of a special authority for the protection of personal data, the Hungarian authority for data protection and freedom of information (NAIH).

The inviolability of privacy and of the home can primarily be ensured through the legislative obligations incumbent on the state, the main instruments of which are civil law, criminal law, and data protection. At the same time, the protection of privacy is also linked to other fundamental rights, most closely to the right to human dignity which, according to the Hungarian Constitutional Court (CC, Alkotmánybíróság) it is one of the constituent elements of.[14]

Art. VI (1) of the Fundamental Law was amended by the Seventh Amendment of the Fundamental Law in 2018 to include an additional sentence that responds to the challenges of digitalization while complying with the protection enshrined in Art. 7 of the Charter of Fundamental Rights of the European Union (EU). This amendment aimed to resolve, at the constitutional level, certain possible conflicts between privacy and other fundamental rights, specifically mentioning the exercise of freedom of expression and assembly as possible limits on the protection of privacy. At the same time, the amendment to the Fundamental Law also established a framework for the exercise of the freedom of expression and assembly, by specifying the right to respect for privacy, family life and the home, thus emphasizing their increased level of protection.

## 4. Civil law

### *4.1. Disclosure of confidential information, protection of private life*

Act V of 2013 on the Civil Code elevated the general protection of private life to a specific personality right,[15] in addition to the other established rights also related to privacy, but with a narrower scope (protection of private dwelling, protection of private information, protection of personal data, the right to one's name, the right to the protection of one's image and voice recording). In fact, the right to private

14 See decision of the Constitutional Court no. 1115/B/1995.
15 Art. 2:43 b) of the Civil Code.

life private law context—media-related cases included—can rarely be accorded an independent meaning which goes beyond the protection of the private dwelling and of one's image, voice recordings, personal data, and private communications. If it is given such a meaning, however, the right to privacy may play a niche role in relation to these established personality rights. Thus, in the Hungarian civil law system of the protection of personality rights, it seems to be the correct approach if the right to privacy does not have independent, *sui generis* content and interpretation beyond this gap-filling role.[16]

Art. 2:44 of the Civil Code establishes, as a basic principle, the limited assertion of the personality rights of public figures in the interests of the freedom to discuss public affairs. According to the provisions which have been in effect since August 2018,

> [Protection of the personality rights of public figures]
> (1) The exercise of fundamental rights ensuring a free discussion of public affairs may limit the personality rights of public figures to an extent that is necessary and proportionate and is without prejudice to human dignity; however, it shall not violate their private and family life and home.
> (2) Public figures shall be entitled to the same protection as non-public figures regarding communications or conduct falling outside the scope of free discussion of public affairs.
> (3) Activities and data in relation to the private or family life of public figures shall not qualify as public affairs.[17]

Art. 2:44 applies to all personality rights relevant to the discussion of public affairs, and thus also affects the interpretation of public figures' rights to privacy, to their image, to their voice recordings and to private information. Act LIII of 2018 ("on the protection of private life") also applies to the protection of these rights. According to Art. 8(1) of the Act, "The purpose of the right to respect for privacy is especially the right to a name, the protection of personal data, private information, image and sound recording, honor and good reputation." Art. 7(2) of the 2018 Act, however, stipulates that the "private and family life, as well as the home of a public figure, shall be granted the same protection as those of a person who does not qualify as a public figure." From reading the two provisions concurrently, it may also be concluded that the right to reputation and honor, as well as the right to one's image and to control over one's recorded sound, are part of the right to privacy and thus the scope of these rights of public figures are the same as the scope of the rights of private individuals.

In reality, however, this interpretation is not acceptable: on the one hand—as we shall see from case law—in terms of the enforcement of these rights, the category

16 Menyhárd, 2014, p. 224.
17 Art. 2:44 of the Civil Code.

of primary relevance is not that of the *public figure*, but of the *public affair*. On the other hand, the same 2018 Act amended Art. 2:44 of the Civil Code (with the content quoted above), which stipulates the restriction of personality rights in the context of the discussion of public affairs. Nevertheless, the new act does not introduce any new tort which may have an impact on the tests of the freedom of speech in the discussion of public affairs, hence it remains possible to establish a violation of "good reputation" or "privacy" only by taking into account the provisions of the Civil Code and the case law which develops based on them. In contrast, the new law defines separate offences of the violation of the right to respect for family life, home and relationships.

The Civil Code primarily protects individuals against the disclosure of confidential information through the protection of confidentiality[18] and the provision on data protection.[19]

The case law published to date connected to the conflict between the protection of confidential information and the right to freedom of the press is not very extensive. Decision no. BH2002. 89 states that "personal data concerning family relations constitute private information." This decision settled a case that was initiated after a newspaper published an interview with the plaintiff's partner and, in the accompanying text, provided the plaintiff's personal details and other information about their family members. The defendants (the editor-in-chief and the publisher of the journal) argued without success that the plaintiff's partner—that is, the interviewee—consented to the publication of the relevant information. This fact—which later turned out to be false—was irrelevant: for the publication of personal data concerning more than one person, the consent of all affected persons must be obtained. Each person concerned may dispose of their personal data only. Having failed to acquire such consent to publication, the journal did in fact breach the personality rights of the plaintiff, and was therefore ordered to compensate the plaintiff.

The personality right to inviolability of the private dwelling may also be relevant for the media. It may constitute a violation of this right if a person lives under the threat of being photographed or of having their voice recorded in their own home or garden without their consent.[20] The Civil Code also protects the right to private information, stating that the

> protection of private information extends in particular to the protection of correspondence, official secrets and business secrets. In particular, the unauthorized acquisition and use, disclosure, or communication of private information to an unauthorized person constitutes a breach of private information.[21]

18 Art. 2:46 of the Civil Code—right to protection of private information; see also Act LIV of 2018 on the Protection of Business Secrets.

19 Art. 2:43 e) of the Civil Code—violation of the right to protection of personal data.

20 BDT2016. 3489.

21 Art. 2:46 of the Civil Code.

The protection of private life has become an autonomous personality right in the Civil Code,[22] the independent content of which is shaped by the judicial practice. The scope of this personality right must also be determined considering the interest of an open debate on public affairs, as must the right to the protection of personal data, which necessarily overlaps with the general right to privacy.[23]

In connection with a fraud scandal which erupted in relation to the Quaestor Group (which led to the bankruptcy of the private financial institution), the same individual was involved in seven CC decisions as applicant.[24] The applicant worked for Quaestor in a relatively minor position, and his partner was the daughter of the attorney general. Publishers of newspapers, television media service providers, and Internet news portals, which had previously been sued, published articles about the Quaestor scandal, in which they disclosed the applicant's name, previous job, the fact of cohabitation with and the name of his partner and the family relations of his partner, as well as information on his wider family through this cohabitation, without the consent of the applicant. The articles insinuated from this information that the alleged delay in the prosecutor's action in the case may have been related to these work-related and family relations. (The articles did not try to prove the truthfulness of this line of thinking.)

In earlier decisions, the Kúria (the supreme court of Hungary) had upheld previous court judgments that dismissed in their entirety a claim for establishing a violation of personality rights related to privacy and the protection of personal data, with one exception, in which the CC turned down the complaint, since the courts of first and second instance established the violation of the right to privacy and personal data protection, which was also maintained by the Kúria[25] In this latter decision, the courts found the disclosure of the applicant's name to have been unlawful and found that the disclosure of the fact of his partnership and the partner's family relations did not infringe the applicant's right to privacy. The CC shared this opinion, and stated that all decisions involving public affairs, while considering the importance of the public matter, may necessitate the restriction of the right of an applicant who is not a public figure to the protection of his personal data[26] for simplicity's sake I will refer below to the first decision only, as the reasoning was essentially identical in all of them.

As far as the publication of the applicant's name is concerned, it was found that the appropriate information could have been provided through reporting without mentioning any names (i.e., anonymously), so the conduct of the press had violated

22 Art. 2:43 b) of the Civil Code.

23 On the interpretation and possible content of the "right to privacy" as a personality right see Ibid.; and see Görög, 2016.

24 3209/2020. (VI.19.) AB; 3210/2020. (VI.19.) AB; 3211/2020. (VI.19.) AB; 3212/2020. (VI.19.) AB; 3213/2020. (VI.19.) AB; 3214/2020. (VI.19.) AB; 3215/2020. (VI.19.) AB.

25 3214/2020. (VI.19.) AB.

26 3209/2020. (VI.19.) AB para. 48.

the privacy of the applicant.[27] The disclosure of his previous job without his consent was not considered a violation, however.[28] The applicant's work relationship with the head of Quaestor, as well as the applicant's private relationship with the attorney general, qualify as "personal data relating to a matter of public interest, the disclosure of which cannot be considered arbitrary or unreasonable disclosure; it enjoys a higher level of protection of freedom of opinion".[29] Regarding the reporting on family relations, the CC also attributed more weight to the task of informing the press about the protection of privacy.[30]

The applicant of decision 3308/2020. (VI. 24.) AB was the secretary general of a children's holiday foundation, about whom an article was published which included an image and video of the luxury villa he rented, its garden and a car with a covered license plate, as an illustration. The CC stated that "freedom of the press does not give a general authority to photograph the property of others".[31] The rights related to the home and the private dwelling are constitutionally protected, according to Art. VI (1) of the Fundamental Law. However, this provision does not protect the property itself, but instead the privacy of the individual.[32] Even so, the published images did not depict anything that could be linked to privacy; moreover, the owner of the rented property had previously made the address of the property and the pictures taken of it available. "The applicant chose the holiday home as a temporary location for his private life, in the knowledge that there are available recordings of it. He may not rely on the violation of privacy due to the re-publication of similar recordings."[33]

As I mentioned above, protection of privacy should be interpreted in the light of the interest in open debate on public affairs. A public figure's private life may be protected, even if what happens in it is partially related to their activities in public affairs:

> I. The right of politicians to have a private life may also be restricted on the grounds of a legitimate public interest and only if the interference is related to the public activities, the ideas promoted, and the acts and statements of the person who has an impact on public life.
> II. The rebuttal of a statement made in relation to an insignificant element of a public event of high interest to the public does not constitute adequate grounds for the press to publish an event regarding the most intimate private sphere of the public figure, an artificial intrusion into the private sphere: exercising the freedom of the press in

27 3209/2020. (VI.19.) AB paras. 51, 52.
28 3209/2020. (VI.19.) AB para. 54.
29 3209/2020. (VI.19.) AB para. 57.
30 3209/2020. (VI.19.) AB para. 60.
31 3209/2020. (VI.19.) AB para. 34.
32 3209/2020. (VI.19.) AB para. 36.
33 3209/2020. (VI.19.) AB para. 36.

such a manner is not proportionate to the violation of the personality rights of the public figure concerned in terms of privacy.[34]

### *4.2. Disclosure of identity*

Disclosure of identity can lead to a breach of privacy in several different situations. For example, victims of accidents and crime have an overriding interest in having their identity kept secret. To facilitate reintegration into the community, the fact of a person's past offences and the punishment they have received should only be disclosed in certain justified situations. There can be an interest in concealing the identity of a person in pending court proceedings, whether as a witness or as a defendant. Finally, it is also possible that someone may be identified "accidentally"; that is, they become identifiable to those around them in such a way that the published article, photograph, etc., does not actually refer to them, and a misunderstanding arises because of similarity of likeness or identical names.

Based on the general right to protect one's name,[35] in addition to the possible infringement of a person's right to bear a name, but mostly beyond that, the infringement of privacy and, often in connection with that, the infringement of reputation and honor is often also raised.[36] Decision BH2002. 221 awarded non-pecuniary damages for a breach of the dignity of the dead and the bereaved to the widow of a security guard who died because of a fight in a nightclub, after a daily newspaper had published the full name, place of residence, and age of the deceased. The Court found that the publication infringed the surviving right to the deceased's good reputation, while it is also clear that the widow's right to undisturbed privacy was also protected by the decision.

"Incidental" identification was the subject of case BH2004.103. The newspaper published by the defendant in this case reported that members of a couple "go to great lengths to keep their erotic relationships fresh." The article reported on K. F. (marked by his initials), a forty-two-year-old mail carrier, who lived in the municipality of "K" and who was allegedly the paper's informant on the subject. The article went on to detail the strange sexual habits of K. F. and his wife. The plaintiff and his wife, who was also identifiable from the article, brought an action against the publisher. In the lawsuit, the defendant argued that the newspaper article was a verbatim translation of an article previously published in an Austrian newspaper, and that only certain details had been adapted to Hungarian circumstances. In addition, he also argued that there are seven post offices in the mail carrier's place of residence (K.), with a total of about one hundred mail carriers working there, so that misidentification was not possible. The Supreme Court, however, upheld the final

34 BDT2018. 3847.
35 Art. 2:49 of the Civil Code.
36 Navratyil, 2014, p. 108.

and enforceable decision, which found that the article was defamatory, because the data published had made identification possible.

The proceedings that preceded decision BH2005.426 were initiated by a person whose name and image were repeatedly published by the police after the infamous 2002 massacre in a bank branch in Mór (a small town near Budapest), describing him as a "person who may be linked to the crime." Although the final and enforceable decision dismissed the action for defamation, the Supreme Court finally awarded damages to the plaintiff for the violation of his personality rights. Although the statement of reasons rightly stated that the phrase "may be linked" is defamatory, as it implicitly refers to his capacity as the perpetrator, the public interest in the speedy investigation of a particularly heinous crime was not sufficiently emphasized in the judgment.

According to judicial practice, a media outlet may report objectively on the status of a criminal procedure by publishing the name of the person concerned.[37] The requirement is that the report must be in line with the current state of the proceedings and respect the constitutional principle of the presumption of innocence. A further question, concerning pictorial representation, is whether a press report may be accompanied by a pictorial illustration showing him or her in an unduly humiliating position.[38]

### *4.3. The protection of one's image and voice recordings*

#### *4.3.1. Requirement of consent*

According to Art. 2:48 of the Civil Code:

> (1) Making and using of a person's image or voice recording shall require the consent of the person concerned.
> (2) The consent of the person concerned shall not be required for recording his image or voice and for the use of such a recording if the recording was made of a crowd or of an appearance in public life.[39]

The subject matter protected by the right to one's image is the human image and its recording using any technology. It should also be noted that, according to the case law, the right to the protection of one's image does not only include the protection of the portrait image: "[I]f the combined presentation of the person's upper body and voice creates a direct link between the person concerned and the criminal proceedings in which they are involved," an infringement is established.[40]

37 ÍH2016.13.
38 3313/2017. (XI.30.) AB.
39 Art. 2:48 of the Civil Code.
40 BDT2015. 3359.

Similarly, a distinctive tattoo, for example, may be capable of identification in public.[41]

According to the relevant section of the former Civil Code (of 1959), the permission of the person concerned was not required for making the recording, although the Supreme Court had already ruled earlier, in BH1985. 57, that the infringement of the right to one's image and voice recording can be committed not only by unauthorized disclosure, but also by making the recording without permission. Likewise, according to BH2008. 266, the "making of a voice recording without permission constitutes an abuse in itself. The burden of proving that making the voice recording was not abusive is on the offender."

A principle has emerged because of the development of judicial law—although it is not contained in the Civil Code—according to which

> a party may not successfully plead a violation of their subjective rights (misuse of their voice recording) if they seek to use this enforcement to conceal their untrue or false statement of facts and seeks to prevent the use of their statement of the truth by relying on their personal rights.[42]

This principle can also be extended to the interpretation of the right to one's image, as was partly done in BDT2011. 2442:

> The making or use of an image or sound recording shall not constitute a misuse if it is made in the public interest or for a legitimate private purpose to prove an infringement that is imminent or has already occurred, provided that making or using the image or sound recording does not cause disproportionate harm as compared to the infringement sought to be proved.[43]

In the absence of statutory exceptions, it can generally be stated that the use of images and sound recordings requires the consent of the data subject in each case (including images freely available on the Internet) and that the consent granted may not be construed in a broad sense[44]. At the same time, consent to taking a photograph or a voice recording can also be expressed by implied conduct—that is, by not objecting to the recording being made after having noticed it.[45] Naturally, it is a violation of the right to image if a person's portrait, otherwise taken with their consent, is mounted on a naked female body, thus giving the impression that the plaintiff (a school teacher) is in the picture, after which the picture is distributed.[46] According to

41 See for instance, decision no. Pf.II.20.286/2011/2 of the Szeged Court of Appeal.
42 BDT2009. 2126.
43 BDT2011. 2442.
44 For example BDT2009. 1962; BDT2007. 1682.
45 BDT2019. 4001.
46 BDT2011. 2549.

the decisions of the Supreme Court[47] settling proceedings related to the publication of the caricatures, publication of an image that does not offend human dignity and is not "unduly offensive or humiliating" is allowed—although the standard of "offensiveness" is constantly changing. These cases do not answer the questions about the boundaries of the privacy of public figures, however. The right to the expression of an opinion may lead to the recognition of exceptions to the requirement of having permission to publish images or recordings of an individual: if an image made in the context of public activities is used as a political message by another person, it shall not be considered as a violation of the law.[48]

#### *4.3.2. Recordings of a crowd*

The lawfulness of using photographs taken at mass events may be a matter of debate. According to the strict interpretation, if a person can be identified in an "image made at a mass gathering," their permission is required to take the picture. According to a more realistic, permissive interpretation, an "image made at a mass gathering" is a photograph of a group of people attending an event, where the identification of the individual participants is only incidental and the photograph is not taken with the purpose of capturing any specific individual. The lawfulness of taking "images made at mass gatherings" and the use of such photos is not disputed in judicial practice today, since no such actions have been brought before the courts recently and, because of this, it is not in itself prejudicial if someone can be identified in such an image without having expressly consented to it being taken or published.

#### *4.3.3. Appearance in public life*

In everyday life, the press interprets the criterion of public appearance in a broad sense: it does not usually ask for consent for the use of images of public figures in public places. In BH1997. 578, the court established that persons attending public events—even as passive observers—waive their right to privacy to a certain extent. Even in such cases, though, images may not be published in an abusive or harmful manner. However, no permission is required for taking pictures—otherwise not harmful—that focus particular attention on individual persons in the crowd and thereby make such persons identifiable. Active participants in public events (for instance, speakers) are unquestionably public figures, while passive observers are not public figures, although the images taken of such observers can be made public (but not misused).

According to BH2006. 282, "The image of a public figure may only be used without their consent in relation to their public appearances and in the context of their public activities, to present such activities. Images of public figures are therefore

47 BH1994. 127; BH2000. 293.
48 ÍH2015. 99.

not freely usable." In this particular case, a satirical magazine used the plaintiff's image independently of and separately from his activities as a public figure; the court found this use to be prejudicial (but did not award damages due to the lack of harm caused by the infringement). According to BDT2007.1663, for

> the purposes of taking images or making voice recordings, the conditions of public appearance are fulfilled if the image or recording is made at a public event where filming and television recording are customary, meaning that anyone attending the event must expect to be recorded—in a recognizable way.[49]

The criteria for public appearance (as part of the public figure's public affairs-related activity) were also defined by the Kúria in its "Criminal–Administrative–Labor–Civil Law uniformity decision" (BKMPJE) no. 1/2012. Accordingly,

> public appearance is considered to be a political, social, artistic activity or expression based on the voluntary and autonomous decision of the individual, which is carried out to achieve a specific goal, in a narrower or broader sense, to influence the life of the local community or society. Therefore…it presupposes an intention to do so on the part of the person appearing in public.[50]

Public figures usually appear in public of their own free will, but this is not always the case. I would therefore disagree with the findings of the judgment published in BDT1999.4 and with those of decision 1/2012. BKMPJE of the Kúria, which state that the concept of public appearance must be voluntary and intentional ("a public figure is one who comes out in public with the desire to act publicly in public affairs"). If, for example, someone is a passive participant in a demonstration that is broken up by the police, and they receive a few truncheon blows in the process, the pictures of that incident can be published without their consent, given the weight of the public interest in publishing them, and as a result the person concerned becomes a public figure against their will. (Of course, the use of the image must not be abusive or offensive, and must not misrepresent any passive, innocent protester, etc.) Similarly, the Norwegian seal hunters became unwilling media actors because their activities concerned a public affairs issue.[51] In actual fact, it is not the status of the person, but their involvement in public affairs that is decisive so from this point of view it is a secondary question whether police officers, seal hunters, demonstrators, etc., are classified by judicial practice as public figures (in the case of police officers this would certainly not be correct), because if their activities are related to the public affairs discussed in public, they will be afforded only reduced protection of their personality rights, including

49 BDT2007. 1663.
50 1/2012. of BKMPJE.
51 Bladet Tromsø and Stensaas v. Norway, app. no. 21980/93, judgment of May 20, 1999.

the protection of their images and voice recordings, regardless of their personal status.

According to the court, however,

> the act of releasing information by a police executive to members of the press on police work qualifies as public appearance. For this reason, using an image of the person delivering such information without permission as an annex to an article discussing the released information does not constitute any violation of personality rights[52].

#### *4.3.4. Extension of the statutory exceptions: Protection of the right to discuss public affairs*

The press previously often published still and moving images in which law enforcement officers may be seen with an uncovered face and can be recognized. These recordings accompany reports on matters of public interest, but the image of the police officers in itself is not newsworthy. At the same time, the persons concerned may consider the publication of these recordings as a violation of their right to their images and privacy, emphasizing that their recognizable representation does not carry any additional information; it does not "add" anything to the merit of the public affairs report's content they illustrate.

Constitutional Court decision 28/2014. (IX. 29.) AB was the first to attempt to strike a balance between the conflicting rights to image and freedom of expression in the context of recordings made of the police. In the specific case at hand, an Internet news portal published an article with an associated "image gallery." In two items in this collection of images, two police officers could be seen in a uniquely identifiable manner, in group photos which also depicted others. The police officers were carrying out their duty, securing the demonstration and standing passively in the picture; their behavior was not or could not be regarded by the press as extraordinary for any reason. These images did not add any additional information to the coverage, nor did they depict the police officers concerned in an offensive, hurtful, demeaning, or distorted way.

It is important to note that the CC did not try to force the facts of the case to fit any of the exemptions provided for in the Civil Code. The images challenged were not mass images, and the CC avoided classifying the work performed and the service provided by the police in public areas as "appearance in public life," since it cannot be considered as such. Earlier, the Supreme Court's uniformity decision had argued, through the lack of public figure status, in favor of the protection of police images but, as a rule, a police officer is not a public figure, although he exercises state powers, and his work in public is not public appearance.[53]

52 BDT2006. 1298.

53 For an argument against the public figure status of police officers, see Pokrócos, 2019.

However, the coverage of a police officer's or other law enforcement worker's activities conceptually affects public affairs, precisely because of the transparency and criticism of the exercise of state powers, therefore it is not sufficient to prove that they are not public figures.[54] The CC upheld with general validity (that is to say, not only for law enforcement officers but generally in relation to those exercising state powers), that their image can be freely published if "the non-offensive footage taken in a public space, depicting the person concerned objectively, may normally be made public without authorization if it relates to a report of public interest and is linked to information on contemporary events".[55] This is how images of police action should also be assessed.[56] The Kúria finally accepted this approach:

> If the person exercising state powers acts in the course of events influencing the public sphere, the exercise of his personality rights relating to his image and their restrictability might be subjected to rules that are different from those pertaining to the general protection of the personality rights of private persons solely participating in public events.[57]

Following this decision, therefore, constitutional aspects related to free reporting and access to information, that is freedom of opinion and of the press, should also be included in the interpretation of the Civil Code. For a while, the CC and the Kúria have not considered this aspect uniformly in individual cases, as evidenced by recent CC decisions adopted upon genuine constitutional complaints, which have reaffirmed the importance of considering the public interest aspect.[58]

As the Kúria also declared the communication of the images unlawful in a subsequent judgment following the decision by the CC, the case was again brought before the CC. The Kúria assumed that the disclosure of an image of police officers standing passively did not carry any additional information, so, because of the deliberation prescribed by the CC, the Court quite reasonably concluded that the disclosure of these images was not necessary for the purposes of proper information, and therefore it was unlawful. However, this is a misinterpretation of the decision made by the CC, as made clear in 3/2017 (II. 25.) AB. The starting point is not that the individual's right to their image is suppressed only in the event of communicating additional information, relevant for the information activity; on the contrary, it can only be enforced if the communication is abusive, self-serving, and distorted. Therefore, the presumption is that the disclosure of images of police officers in connection with reporting on a public event is permitted.

54 Regarding the constitutional issues inherent in the issue, see Balogh and Hegyi, 2014; Somody, 2016.
55 Para. 44.
56 Para. 43.
57 BKMPJE decision 1/2015, para. IV.3.
58 See 16/2016. (X.20.) AB and 17/2016. (X.20.) AB.

In the event of such circumstances, the courts may examine, in the case of a press body falling within the scope of the Press Freedom Act[59] and the Media Act,[60] the fairness and good faith of the coverage as a whole, during which the parties must be granted the opportunity to make statements and to substantiate and refute them by evidence. However, if such a circumstance did not arise, as was never the case at hand, since the plaintiffs did not state that the coverage had represented their presence and role in the event covered by the report falsely, and therefore as an end in itself, the courts are required to enforce the primacy of the constitutional interest in the presentation of contemporary events, in line with the scope of interpretation set out in 28/2014. (IX. 29.) AB.[61]

Representatives of other professions may also be photographed at public spaces against their will. Constitutional Court decision 3021/2018. (I. 26.) concerned the image rights of legal representatives acting at a trial, who were legal counsels representing the police in litigation. At the hearing, the legal counsels did not consent to photos being taken of them and the court subsequently ruled that a recording of the image and sound could only be made of the plaintiff's side and of the court itself. However, one of the applicants in the CC decision made recordings in which the solicitors were individually identifiable. A printed version of the judgment, which also included the names of the legal representatives, was presented in a recording published later, accompanied by the following commentary: "What is shocking, indeed, is the way in which the Pintér police [Sándor Pintér being the Minister of the Interior] are being defended in a sly and, let's say, unprincipled way by their legal counsels."

The CC saw no reason to annul the Kúria's decision, which had found both the preparation and publication of the recording to be infringing. A decisive factor was that the recordings were made at a court hearing, the disclosure of which is subject to special rules, and that, based on these rules, the acting judge lawfully prohibited the recording from being made, by making an order.[62] Both the context and the role of those affected distinguishes this case from police image cases; "the recording and disclosure of images despite the prohibition of a court order, in the absence of a manifest unfoundedness of the judicial discretion, cannot be considered a proper, non-abusive exercise of press freedom".[63]

The applicant in 23/2019. (VI. 18.) AB was a television broadcaster who carried a report in its news program about a trial pending before the Kúria, presenting footage in which it did not cover up the face of the law-enforcement worker accompanying the accused, and showing him in a recognizable way. In this case, the CC had to determine an important point, different from the facts of the case in the police officers' image cases: can the image of a person exercising state power, present at a court

59 Act CIV of 2010 on the Freedom of the Press and the Fundamental Rules of Media Content.

60 Act CLXXXV of 2010 on Media Services and Mass Media.

61 3/2017. (II. 25.) AB, Para. [25]. For a comprehensive overview of police image cases and the issues raised by them, see Fejes, 2017; Sándor, 2020; Tóth, 2017.

62 Para. 24.

63 Para. 30.

hearing, i.e., not in a public place, be disclosed as part of audiovisual coverage?[64] The panel established that the court decisions in the case at hand were based on the protection of the right to image, but at the same time it did not identify any element of the coverage that would have violated the dignity of the person concerned. Specifically, it found that

> the pictorial representation of the activity of a person exercising state power in this capacity is restricted only if there is a special constitutional reason for it. The administration of justice and the independence of the judiciary may justify a restriction on freedom of the press in the courtroom, but becoming recognizable is not such a reason in itself. No person exercising state powers—in accordance with the conclusions drawn in 28/2014. (IX. 29.) AB—may rely on the protection of human dignity at a court hearing only because he becomes recognizable in media content.[65]

The case law of the CC also extends to constitutional issues related to the disclosure of the image of public and political figures. Based on 3313/2017. (XI. 30.) AB, an image taken of a political figure present in a courtroom as the accused person, even if he was acquitted in subsequent proceedings, may be of high interest to the public and is linked to the status of the accused as a public figure. The media may objectively report—including by visual means—on the state of play of criminal proceedings, providing the news coverage reflects the status of the given proceedings and respects the assumption of innocence as a fundamental constitutional principle. Visual representation in itself does not violate this principle, nor does the depiction of physical means of coercion (handcuffs) used against the accused constitute abusive or degrading treatment to begin with.[66] The motion alleging a violation of personality rights was accordingly turned down by the CC.

Decision 3348/2018. (XI. 12.) AB arose following the disclosure of another accused political public figure. As an illustration to an article on an Internet news portal, the applicant used a photograph of the person that had been previously taken for another news portal during a criminal prosecution. An important circumstance is that, following the publication of the image, the public figure concerned won a civil lawsuit against the news portal that took the image, successfully prosecuting the site for abuse of his image. However, in this case, the CC stated that the constitutionality of the use of the image in the specific case may nevertheless be examined separately.[67] The image was closely related to the content of the newer article and the court proceedings of public interest presented in it, which were related to the public figure quality and position of the former politician. Furthermore, the image did not depict him in a humiliating situation, or in a way that would seriously hurt

64 Paras. 29, 30.
65 Para. 41.
66 Paras. 51, 62.
67 Para. 36.

or violate the unrestricted essence of human dignity.[68] Accordingly, the publication of the image did not constitute an abuse of the right to freedom of the press, hence the judgment of the Court of Appeal which had established such a violation was therefore contrary to the Fundamental Law.[69]

In the case that led to 26/2019. (VI. 23.) AB, footage of a political adviser keen to avoid publicity, was taken of him while he was on holiday abroad. The recording—made for a promotional video—was commissioned by the nightclub he had visited. An important circumstance was that, in accordance with the general terms and conditions of the establishment, the consultant consented to the production of a recording, including the use of his image for advertising purposes, which the nightclub used in the course of its own activities. These recordings were republished by a Hungarian online news portal. The CC rejected the constitutional complaint because the report on the consultant's holiday was a public matter, and if

> the press publishes an image in a matter related to public discourse, the "protection of image" may only be a genuine restriction of press freedom if the publication of the image violates a fundamental right beyond becoming recognizable (in particular a violation of human dignity or the right to privacy).[70]

The article and its pictorial illustration were not defamatory or insulting, and

> the press shared media content about the privacy of an individual who has an impact on public life in connection with debating public affairs. Since, in this case, the subject of a democratic debate was privacy itself (the financial situation and lifestyle of the person concerned), and the applicant had consented to it being recorded and shared it for promotional purposes, the court correctly interpreted that sharing this information with the public does not entail the violation of human dignity or the right to privacy.[71]

One of the applicants in 3467/2020. (XII. 22.) AB was a politician and the other one was his spouse, who is not a public figure. The challenged court decision rejected their claim for the protection of their right to their images. In this case, an online news portal posted photos of the politician as well as a profile picture attached to his social media account, depicting him and his spouse. The CC established that none of the images of the politician could be considered a depiction of a private event.[72] Although the wife could justifiably allege a violation of her rights to privacy in the event of her image being published, in the specific case at hand she did not become

68 Para. 37.
69 Para. 38.
70 Para. 40.
71 Para. 42.
72 Para. 69.

recognizable in the profile picture, due to its small size and the impossibility of magnifying it, so her fundamental rights were not violated.[73]

Decision 3019/2021. (I. 28.) AB was adopted after an online portal published an article analyzing the relationship of a family to the mayor of a town, as well as the evolution of the family members" financial situation. The article was illustrated with images of the mayor and various members of the family, originating from other media providers.[74] The courts found a violation of the right to image. An important criterion in the CC's decision was that the images published were not created to illustrate the article, but on the occasion of an earlier public appearance. However, the content of the article concerned public affairs.[75] After due consideration, the CC accepted the constitutionality of the decision delivered by the courts, which "in cases where the image is not related to the public speech to which the communication relates, makes the disclosure of the image conditional on the consent of the person concerned who does not exercise state powers".[76] The CC turned down the application for annulment.

In the meantime, the practice of ordinary courts in connection with the right to the protection of one's image has also shifted in favor of considering the interests of the public in a variety of different life situations, expanding the scope of exceptions afforded under the Civil Code and narrowing the scope of the right to the protection of one's image accordingly: "If somebody accompanying a public figure participates in an event which is financed from public funds, he or she might expect the media to report on that, even using his image".[77]

> I. If the representatives of the press are not granted access to an event with limited access to the press and the related prohibition is communicated by the designated person representing the press department of the public authority in the lobby of the building, the press reporting on this by publishing audio and video recordings shall not be obliged to pixelate the face of the civil servant speaking on behalf of the public authority.
> II. The pixilation of the face may essentially impact the credibility of the news report, worthy of public attention, on the event and would therefore disproportionately restrict information on current events and the freedom of the press.
> III. The civil servant performing communication-related tasks shall be obliged to tolerate the publication of his image and recorded voice with respect to an event worthy of public attention to ensure the freedom of discussing public affairs. The fundamental right of the press to the freedom of expression may restrict—to the necessary and proportionate degree—the personality rights of the representative of the public authority to his image and recorded voice.[78]

73 Para. 72.
74 Para. 2.
75 Para. 36.
76 Para. 38.
77 BH2017. 86.
78 ÍH2018. 52.

At the same time, a matter in the public sphere and the in interests of the media may not restrict the enforcement of personality rights disproportionately. Recordings made with hidden cameras may be legitimate only in exceptionally justified cases and public figures may be subjects of recordings only "in situations that are of high interest to the public."

> I. The information obligation of the press does not create privileges; linear media services are obliged to conform to legislative provisions while meeting this obligation and, as a main rule, their activities may not infringe upon others' personality rights. In the case of a video or audio recording made of a public figure without his consent, in a public place, the collision between the freedom of opinion and the protection of personality rights needs to be resolved by weighing up interests, even if the statement or publication otherwise contributes to informing the public of an affair which is of high interest to them.
> II. The usage of a recording made with a hidden camera violates the right of the public figure to his image and recorded voice if the statements recorded do not contribute to the debate of the affair of high interest to the public, or if they are not informative in a way that would stimulate this debate.[79]

> I. The publication of a recording made of a public figure may restrict the right of the public figure to his image protected by law only to the degree that is necessary and proportionate to debate public affairs.
> II. An image of a public figure taken in a situation which is not of interest to the public may only be published with the consent of the person concerned. In the absence of such consent, the image taken of him and published violates the right of the person concerned to his image, in the protection of which the injured person may file a lawsuit to enforce this right expressly.[80]

An action was filed for the violation of the right to the dignity of the dead and the bereaved by the publication of images of the corpse of the celebrity singer Jimmy Zámbó, who died in tragic circumstances.[81] The tabloid article on this event was accompanied by pictures of the body taken after the autopsy. The task of the court was to decide whether the publication of such images amounts to defamation of the deceased, thereby constituting a violation of the right to dignity. According to the final decision of the court, rights to dignity were not violated by the mere publication of the images, as "the fact and portrayal of one's death is not capable of having any negative impact on the social standing of the deceased." However, the Supreme Court did not concur, and stated that displaying a corpse "after autopsy, under humiliating

79 BDT2017. 3760.
80 BDT2017. 3693.
81 EBH2005. 1194.

circumstances, and in a condition giving rise to regret" is in itself capable of harming the honor of the deceased.

The point made in the decision, that the deceased "created a dynamic, attractive, positive image of himself in many people's minds [while] the photograph, on the other hand, shows him in a completely vulnerable position, in humiliating circumstances and in a physical state that arouses pity", thus increasing the danger of the act to society is questionable. In such a situation, the distinction between public figure and private person is hardly justified; indeed, the publication of pictures of the dead bodies of private persons can be equally unlawful.

Nevertheless, tabloids may even get away with material violations, unless an action is filed with the court. Perhaps the most outrageous example of such a violation was that of a tabloid front page photograph (published in 2004) showing the agony of Miklós Fehér, a member of the Hungarian national football team. The picture—which was displayed on the front page of the paper—showed the anguished and sweating face of the football player as he collapsed during a match in Portugal, and died within minutes of the picture being taken. While no court action was filed, the Data Protection Commissioner expressed his objections.[82]

#### *4.3.5. Special litigation proceeding for image protection*

Act CXXX of 2016 on the Code of Civil Procedure allows for a special procedure for the enforcement of the right to the protection of one's images and voice recordings, the primary aim of which is to remedy the infringement as quickly as possible.[83] The enforcement of this right, similar to the right of reply, takes place in two separate stages: the aggrieved party must first send a written request to the producer or user of the image or recording within 30 days of becoming aware of the image or sound recording having been made or used. The request (for which the law sets a three-month limitation period) may ask for an injunction to stop the infringement, for appropriate satisfaction (and publicity at the expense of the person causing the damage), or to remedy the injurious situation, restore the situation prior to the infringement, and eliminate the thing produced by the infringement or deprive it of its infringing character.

If the maker or user of the image or recording does not comply with the request or does not comply with it properly, the person making the request may bring an action, which must be brought within fifteen days of the last day of the period set for remedying the breach specified in the request. The time limit for bringing an action is of a substantive law nature, which means that the statement of claim must reach the court within fifteen days.[84] A further restriction is that the action may only request the application of the sanctions specified in Arts. 2:51(1)(a)–(d) of the Civil

82 Communication no. 135/H/2004.
83 Arts. 502–504 of the Code of Civil Procedure.
84 See BDT2016. 3502.

Code. The law provides for the application of the provisions of the procedural rules for the enforcement of the right of correction in matters not covered by the specific rules for image protection.

It should be noted that if the injured party does not wish to make use of the enforcement options or fails to meet the deadlines, they may initiate a personal rights lawsuit under the general rules. If they do so, the limitation on the range of available sanctions shall not apply either, so that, for example, a person who would like to claim aggravated damages (compensation for injury to feelings) on the grounds of an infringement cannot enforce such a claim under the special procedure.

### *4.4. General civil litigation proceedings*

Art. XXVIII (1) of the Fundamental Law lays down the requirement for the publicity of judicial proceedings (open justice). However, the requirement of publicity as an aspect of the right to a fair trial to allow free provision of information on judicial proceedings cannot be regarded as an unlimited right. When informing the public, the media must also respect other rights. Such rights, which may restrict publicity include the personality rights of the participants in the trial (in particular, the right to the protection of one's image and voice recordings, the right to privacy and the protection of minors).

In civil actions, the relevant rule provides,[85] as an exception to the principle of the publicity of the hearing, that the court may exclude the public from the hearing for the purpose of protecting the personality rights of any party.[86] Similarly to criminal procedures, the legislature and the law enforcement authorities have an especially great responsibility in civil proceedings for striking a delicate balance between publicity and personality rights, and between data protection and confidentiality.[87]

The publicity of the courtroom is also of paramount importance for the press to fulfill its duty to inform the public on public matters. This does not mean, however, that these tasks can be carried out without any restrictions, even in cases of considerable interest, because

> [the] standards for the exercise of freedom of speech and freedom of the press with regard to taking photographs and video recordings differ in the context of courtrooms and trials on the one hand, and other venues (typically public spaces) and public events taking place there on the other. While in the latter case, recording and reporting contemporary events may be restricted only in exceptional cases, detailed legislation may be necessary in the former case, above all to ensure the independence and impartiality of the court, to guarantee the independence of the judgment from any external influence, to ensure the smooth conduct of the proceedings and to

85 Act CXXX of 2016 on the Code of Civil Procedure (hereinafter referred to as Civil Procedure Act).
86 Art. 231, para. 2 of the Civil Procedure Act.
87 Horváth, 2013.

> protect the interests of the parties to the proceedings… The courtroom is not in itself a forum for the discussion of public affairs, but a place of justice where the accusation or the rights of the parties to the proceedings are decided. In the light of the general interests of justice and the specific interests and rights of the parties involved in the trial, the press coverage of the courtroom must therefore be assessed differently, and the restriction of press freedom in this case may be justified in a broader scope than in the case of ordinary reporting on public affairs and current events.[88]

## 5. Criminal law

### *5.1. Disclosure of confidential information, invasion of privacy*

Criminal law provides protection against disclosure of confidential information by defining several actions as criminal offences.[89] The offence of trespassing is intended to protect the right to the undisturbed use of the private dwelling and other premises belonging to the dwelling, as guaranteed by the Fundamental Law.[90] The object of the offence is another person's dwelling, other premises and the fenced-in area belonging to them, or the interest of their undisturbed use.[91]

The breach of private information (breach of confidence) is directed at private information as a legal category.[92] Private information is any confidential fact or information—concerning an individual's personal, family, financial situation, health, or particular habits—known only to a restricted circle or to insiders, the disclosure of which would be prejudicial to the interests of the victim.[93] An offence occurs when the private information is disclosed without good cause, but the offence can only be committed by a person who has obtained the private information by virtue of their profession or public mandate.

The protection of the confidentiality of correspondence is primarily guaranteed by the right to privacy declared in Art. VI of the Fundamental Law, and the right to human dignity declared in Art. II of the Fundamental Law as a personal right. The purpose of this law is to prevent the contents of private messages containing personal intellectual content from becoming known to persons outside the circle of

88 3021/2018. (I.26.) AB para. 26.
89 Art. 221 of the Criminal Code [Act C of 2012 on the Criminal Code]–trespassing; Art. 223—breach of private information; Art. 224—breach of confidentiality of correspondence; Art. 422—illegal acquisition of data; Art. 418—breach of trade secrets; Art. 219—misuse of personal data; Art. 220—misuse of data of public interest
90 Art. VI of the Fundamental Law.
91 BH2019. 97.
92 See also Karsai, 2013, p. 468.
93 BH2004. 170.

the sender(s) and the addressee(s). In addition, this criminal offence is committed by anyone who intercepts a communication transmitted by means of an electronic communications network, which constitutes an act intended to obtain knowledge of the content of the communication during its transmission by means of an electronic communications network. This covers eavesdropping (wiretapping) using virtually any technology.

The prohibition of the illegal acquisition of data primarily seeks to protect the personality right to the protection of private information derived from the right to privacy and the interest in the protection of personal data, business, and trade secrets, as well as the right to the inviolability of the private dwelling and the confidentiality of correspondence and private telecommunications information. It is important to note, however, that this offence is committed only when it is carried out in the (private) dwelling (home) or other premises of another person—but not in a workplace, office premises, or in the common areas of the workplace, such as a camera installed in the bathroom at a workplace.[94] Hence, a person who makes a recording without consent in a place other than the place specified in the criteria of the offence, for example "at the workplace, office premises, or common areas of the workplace," does not commit the offence of illegal acquisition of data.[95]

The illegal acquisition of data committed using a drone is considered a special offence, with a specific nature: that the observation and recording in such cases are conjunctive offences, and that the unauthorized use of unmanned aircraft for observation and recording constitutes the means of the offence itself. Unmanned aircraft are defined in Art. 3 of the Commission Delegated Regulation (EU) 2019/945 of March 12, 2019, on unmanned aircraft systems and third-country operators of unmanned aircraft systems, which defines an unmanned aircraft as any aircraft that operates without a pilot on board or is designed to do so and is capable of operating autonomously or by remote control. This concept is used in Act XCVII of 1995 regulating air traffic and in Government Decree 4/1998 (I. 16.) on the use of Hungarian airspace, which also specifies the legal framework for drone use.

### *5.2. Criminal proceedings*

Among the basic principles of Act XC of 2017 on Criminal Procedure is the requirement to respect human dignity.[96] The Criminal Code stipulates that "the court, the public prosecutor's office and the investigating authority may only allow access to personal data and protected data processed in criminal proceedings in accordance with the provisions of the law",[97] and, during the enforcement of coercive measures, it must also be ensured that "the circumstances of the private life of the person

94 BH2017. 361.
95 BH2017. 361.
96 Art. 2, para. 1 of the Code of Criminal Procedure.
97 Art. 98, para. 2 of the Code of Criminal Procedure.

concerned not related to the criminal proceedings or their personal data are not disclosed".[98] On this basis, preventing the identification of persons under investigation became the main rule.

In criminal proceedings, court hearings are also open to the public as a general rule, and the media can report on them.[99] According to the position of the CC on the publicity of criminal proceedings, publicity is intended to promote social control over the administration of justice (that is, the enforcement of the requirement of transparency and accountability).[100] The principle is that court hearings are public as a general rule, and that anyone can attend as a listener, but this principle does not mean that anyone has a substantive right to attend, that is participation can be restricted or excluded for a well-founded reason. In certain cases, the chair of the court panel may exclude or restrict the public from the hearing, which may be done to protect the interests (including privacy) of the persons involved in the hearing.[101] One of the limits to the principle of the public nature of court hearings is that the law provides that permission to take pictures or audio or video recordings of the hearing may be refused if this would result in an imminent risk to the privacy of the person involved in the criminal proceedings.[102]

In some cases, the law itself provides for the applicability of measures restricting privacy. For example, Art. 214(1) of the Code of Criminal Procedure provides for the possibility of the use of covert/disguised instruments or means, a special activity in criminal proceedings entailing restrictions on the fundamental rights to the inviolability of the private dwelling and to the protection of private information, correspondence and personal data, and which are carried out by the bodies authorized to do so without the knowledge of the person concerned.[103] The use of secret service instruments and methods constitutes a significant intrusion into the private sphere, and it is therefore an essential requirement within the framework of the rule of law that the conditions and framework for the use of such means are laid down by law, with the necessary guarantees and safeguards.[104] In addition to the rights set out in the law, human dignity is also violated in all cases where a person—for example, a person talking on the telephone—is not treated as a person but as an instrument.[105]

It should be noted that the Code of Criminal Procedure has moved the regulations on the secret collection of information for purely law enforcement purposes, carried out by the public prosecutor's office, the police and the National Tax and Customs Administration, from the sectoral rules to the framework of criminal procedure, breaking with the previous regulatory structure. This removed the rule that

98 Art. 271,. para. 5 of the Code of Criminal Procedure.
99 Art. XXVIII, para. 1 of the Fundamental Law; Art. 436 (1) of the Code of Criminal Procedure.
100 58/1995 (IX. 15.) AB, Statement of reasons, para. II.5.
101 Art. 436, para. 4 of the Code of Criminal Procedure.
102 Art. 109, para. 1 a) of the Code of Criminal Procedure.
103 See also Gyaraki and Simon, 2020, pp. 138–140.
104 Bárándy and Enyedi, 2018, p. 97.
105 Korinek, 2019, p. 185.

allowed the results of the most intrusive means of covert information gathering to be used for purposes other than the original purpose of the criminal proceedings.[106] Moreover, the CC has examined certain elements of existing legal provisions and annulled some of them on the grounds that they used vague terms that may have led to further unpredictable interpretation.[107]

## 6. Protection of personal data

Data protection is the result of the development of European, and more specifically continental European law, which was previously governed by radically different rules in the Anglo-Saxon countries, especially in the United States. Its emergence can be linked to the spread of computer-based data processing and the recognition of the dangers of new communication technologies. In the 1960s and 1970s, the large paper-based public registers were gradually replaced by computerized systems. The new technology facilitated much more efficient storage of much larger amounts of data and made it much easier to link and interconnect different registers and records. All this gave the state an informational supremacy that could even bring the realistic possibility of creating an Orwellian world. To protect fundamental democratic values, it became necessary for the state to create limits—primarily for itself—to ensure the protection of its citizens' personal data and, through this, their undisturbed privacy. The aim is to ensure that citizens are "transparent" to other persons—the state and market actors—only to the extent necessary.

Data protection essentially creates a parallel privacy protection; Act CXII of 2011 on the Right to Informational Self-Determination (hereinafter referred to as the Information Act) and the EU's directly applicable General Data Protection Regulation (GDPR)[108] cover the entire scope of protection provided by traditional personality law (any information about the data subject is considered personal data and therefore protected, and taking a picture or making an audio recording is also covered by the concept of data processing), so the protection of private information, private dwelling, image, and sound recording can also be achieved through data protection. This parallelism is also observed in the Civil Code, which deals with the right to the protection of personal data as a personality right.[109] It also allows for the possibility of bringing civil proceedings for essentially any breach of data protection rules.

106 Ibolya, 2015.

107 2/2007. (I.24.) AB.

108 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

109 Art. 2:43 e) of the Civil Code.

Personal data is therefore part of the private sphere, and data protection is a means of protecting the personality and the privacy of individuals. The right to the protection of personal data—as a personal right—can only be exercised by a natural person, meaning that legal entities and organizations without legal personality cannot exercise such a right. Deceased persons do not have such a right either, hence their relatives can make such claims instead only under the right to the dignity of the dead and the bereaved.

The right to data protection is not just a passive, protective right. In recent years, there has been a growing recognition that the essence of personal data protection lies in the right of data subjects to have control over their personal data. This right of informational self-determination can be compared to the right to dispose of property, so personal data can be understood as a kind of informational property. The data subject is free to decide, subject to certain legal restrictions, whether to disclose, consent to or withdraw consent to the processing of their personal data.

The right to the protection of personal data as a right to informational self-determination was first identified as such by the German Constitutional Court. This interpretation was adopted by the CC when, in its decision 20/1990. (X. 4.) AB, which found that the law on the declaration of assets of certain state and party functionaries was unconstitutional, it stated that the right to the protection of personal data "means that everyone is free to decide on the disclosure and use of their private information and personal data." The decisions taken on this issue in the years following the political transition are the intellectual forerunners of the first Data Protection Act of 1992 (Act LXIII of 1992), which is still widely cited today. In one of the most important decisions on this issue, in 15/1991. (IV. 13.) AB, the CC held that the "collection and processing of personal data for any future use without a specific purpose" and "a universal and uniform personal identification number (personal number) that can be used without restriction" are unconstitutional. Decision 2/1990. (II. 18.) AB found that the application of the proposal coupon (recommendation slip)—on which the name, address, and personal number had to be indicated—introduced by the Electoral Act was compatible with the Constitution. The right to the protection of personal data, like other fundamental rights, is not an absolute right, hence it is not the case that personal data "cannot be disclosed to any person other than the data subject for any reason and under any circumstances." In the same way, it does not follow from the constitutional guarantees of the right to informational self-determination that anyone may formulate a constitutional claim that a body (organization), which otherwise also performs data processing, would be obliged to scan (process) all data stored by it on non-electronic media to facilitate a search for the personal data of the data subject, even though it has not previously performed any operations on them and is not aware of their storage.[110]

The right to informational self-determination can therefore be limited. The general conditions for the restriction of fundamental rights are laid down in Art. I (3)

110 3079/2018. (III.5.) AB.

of the Fundamental Law and these were also developed by the practice of the CC (necessity-proportionality test). Regarding the right to the protection of personal data, the CC has also developed specific guarantees in addition to the general conditions for the restriction of fundamental rights. In this respect, the CC primarily evaluates compliance with the purpose limitation requirement and establishes the existence of a public interest in the disclosure and transmission of personal data. However, in 46/1995. (VI. 30.) AB, the CC ruled that the public interest alone cannot be the basis for a restriction of a fundamental right, but only if the reason for the restriction is stated in the Fundamental Law. Thus, for example, restricting the access of persons with limited capacity to gambling, thereby effectively protecting their personal and property interests, is a constitutionally acceptable objective that adequately justifies the need to restrict the right to the protection of personal data.[111]

This freedom of self-determination was previously guaranteed as a fundamental right for everyone by Directive 95/46/EC of the European Parliament and of the Council, and is currently guaranteed by the GDPR, which entered into force in May 2018. In Hungary, this freedom was guaranteed by the Constitution between 1989 and 2012, and since 2012 by the Fundamental Law. However, the GDPR, created as a result of the 2016 EU data protection reform, and the Criminal Data Protection Directive have fundamentally changed the domestic regulatory environment of data protection rights.[112] In connection with the provisions of the GDPR—as a source of EU law at regulatory level—which entered into force directly, the Hungarian legislature was expected to carry out a comprehensive review of the previously adopted, comprehensive data protection legislation (the Information Act), including the creation of institutional and procedural rules necessary for the implementation of the GDPR, as well as the introduction of possible deregulation measures, the implementation of the rules of the criminal directive and ensuring the consistency of certain sectoral rules with EU rules.[113] (These laws were adopted in July 2018 and, for sectoral rules, in April 2019.) Because of the EU legislation and the domestic legislation adopted in accordance with it, concerning data processing within the scope of the GDPR, only those provisions of the Information Act that are expressly provided for by the law as standards supplementary to the GDPR can be applied (and may be applied; see Art. 2(2) of the Information Act). Consequently, a significant part of the Information Act—a set of provisions affecting the areas covered by the GDPR—has been repealed.

From the point of view of the protection of personal data, some public figures are subject to special treatment (like the application of the provisions on the protection of reputation and of integrity and privacy). Information relating to public figures

111 3046/2016. (III.22.) AB.

112 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

113 Regarding this, see Péterfalvi, Révész and Buzás, 2018, p. 42.

acting on behalf of public bodies and in the exercise of their functions and powers that relates to their activities and the performance of their public interest tasks is data accessible on public interest grounds.[114] In this regard, EBH2000.323 states that "the fact that the natural person to whom the data relate will be considered a public figure years later does not in itself make the personal data…data of public interest." In the case, a historian requested access to former Prime Minister Gyula Horn's Ministry of Finance files (which are possibly related to his activities during the 1956 uprising, when he was a member of the Communist secret police), which the body refused to grant, rightly, according to the court. The past activities of public figures are therefore not necessarily considered to be public if they are not related to their present public activities. A general statement to this effect may be a matter of concern, given that citizens have the right to know everything that may influence their decisions (in the case of the prime minister, for example, their decisions at the next parliamentary elections).

However, a significant part of the data concerning and relating to public figures—which does not qualify as personal data—is public interest data or data accessible on public interest grounds. According to the ombudsman's practice, public data include, for example, the names, titles, jobs, and salaries of civil servants. Similarly, the doctoral dissertations and doctoral thesis of former party leader József Torgyán and former Prime Minister Gyula Horn are freely accessible for research by anyone. The minutes of the Opposition Round Table (in existence in 1989) are data of public interest, even though the Opposition Round Table was not formally a political organization. The names of the top executives of Hungarian Television Ltd. are data of public interest, as are the salaries of the presidents of Hungarian Television Ltd. and Hungarian Radio Ltd. or the National Bank of Hungary.[115]

## 7. Administrative procedures

The constitutional right to fair administration declared in Art. XXIV of the Fundamental Law has been ensured in practice by the legislature within the framework of the legislation in force regulating administrative procedure.[116] The established judicial practice in this area takes into account the relevant resolution of the European Parliament,[117] which cites the principle of respect for privacy under Recommendation No. 3 on the general principles to be respected in administrative proceedings.[118] The

114 Art. 26, para. 2 of the Information Act.
115 Majtényi, 2006, pp. 402; 416–418; 435; 438–439.
116 Act CL of 2016 on the Public Administration Procedures.
117 European Parliament resolution of January 15, 2013, with recommendations to the Commission on a Law of Administrative Procedure of the European Union (2012/2024(INL)).
118 Barabás, Baranyi, and Fazekas, 2018.

law allows for restrictions on the right of access to documents on the grounds of the protection of private information and personal data,[119] while the conflict between the right to a fair procedure guaranteed by the Fundamental Law and the protection of privacy must be resolved by the law enforcement authorities on a case-by-case basis. (In the exercise of the right of access to documents by third parties, the assessment of personal and protected data must also follow the legal provisions of the Information Act on the disclosure of data of public interest.[120])

In the context of clarifying the facts of the case, the law regulates the institution of an official inspection, which enables the authorities to inspect or observe movable property, real estate or persons.[121] When applying this means of gathering evidence, the privacy of the person concerned must be respected, and therefore the "observation" of a person cannot be understood as the secret and continuous observation or surveillance of the person by the authorities since "secret/covert collection of information or data"; that is, the official inspection is not an investigative tool.[122] It should be noted that, in certain procedural acts, the authority may also use an official witness, who may necessarily have access to information relating to the private sphere of the person concerned, to verify the events and facts which it has observed during the procedural act. It is precisely with this in mind that the law stipulates that, as a rule, official witnesses are bound by the obligation of confidentiality regarding the facts and data they become aware of during the procedural act.[123]

## 8. Conclusions

Privacy protection in the Hungarian legal system is implemented in a comprehensive way. In addition to constitutional protection, privacy is specifically protected by many areas of law and by the rules governing the different types of legal proceedings. The most important of these are private law, criminal law, and data protection. Ensuring freedom of expression is also a priority, and its constitutional protection must be considered when applying the rules in all areas of the law. Beyond the rules of law, case law also plays a decisive role, as the case law of the Kúria and the CC help find the appropriate balance between conflicting rights. In this respect, the Hungarian legal system has come a long way since the democratic transformation of 1989/90, and has successfully fulfilled this task, while facing the new challenges posed by the proliferation of new technologies.

119 Art. 34, para. 2 of the General Public Administration Procedures Act.
120 Petrik, 2017, p. 99.
121 Art. 68, para. 1 of the General Public Administration Procedures Act.
122 Barabás, Baranyi, and Fazekas, 2018.
123 Art. 79, para. 4 of the General Public Administration Procedures Act.

# Bibliography


Balás, P. E. (1941) 'A személyiségi jogok' in Szladits, K. (ed.) *Magyar Magánjog I. Általános rész. Személyi jog.* Budapest: Károly Grill, pp. 653–654.

Balogh, A., Hegyi, Sz. (2014) 'A Kúria jogegységi határozata a közhatalmat gyakorlatról készült képmás és hangfelvétel nyilvánosságáról. Közszereplő-e a nyilvános helyen szolgálatot teljesítő rendőr?', *Jogesetek Magyarázata,* 5(2), pp. 29–35.

Barabás, G., Baranyi, B., Fazekas, M. (eds.) (2018) *Kommentár az általános közigazgatási rendtartásról szóló törvényhez*. Budapest: Wolters Kluwer.

Barzó, T., Halász, Cs. (2020) 'Elmosódott magánélet? A privátszféra érvényesülése és határai az online közösségi térben', *Miskolci Jogi Szemle*,15(1), pp. 33-47.

Bárándy, G., Enyedi, K. (2018) 'Leplezett eszközök és titkos információgyűjtés, avagy az új büntetőeljárási törvény margójára', *Büntetőjogi Szemle*, 7(1), pp. 97–104.

Constant, B. (2016) 'The Liberty of the Ancients Compared with that of the Moderns' in Blaug, R., Schwarzmantel, J. (eds.) *Democracy. A Reader.* 2nd edn. New York: Columbia University Press, pp. 108-110; https://doi.org/10.7312/blau17412.

Fejes, E. (2017) 'A rendvédelmi testületek hivatásos állományába tartozó személyek képmáshoz fűződő jogának korlátozhatósága' in Görög, M., Menyhárd, A., Koltay, A. (eds.) *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül.* Budapest: ELTE ÁJK, pp. 143–161.

Gajda, A. (2022) *Seek and Hide. The Tangled History of the Right to Privacy.* New York: Penguin.

Görög, M. (2016) 'A magánélethez való jog mint a személyiségi jog újabb, magánjogi kódexben nevesített vonatkozása' in Balogh, E. (ed.) *Számadás az Alaptörvényről.* Budapest: Magyar Közlöny Lap- és Könyvkiadó, pp. 51–63.

Gyaraki, R., Simon, B. (2020) 'Kiberbűncselekmények felderítése és nyomozása' in Kiss, T. (ed.) *Kibervédelem a bűnügyi tudományokban.* Budapest: Dialóg Campus, pp. 121–150.

Horváth, E. Í. (2013) 'A polgári perek nyilvánossága', *In Medias Res*, 2(2), pp. 381–382.

Ibolya, T. (2015) 'A Jó, a Rossz, és a Csúf, avagy az ügyész, a korrupció elleni küzdelem és a Be.', *Magyar Jog*, 16(5), pp. 312–315.

Karsai, K. (ed.) (2013) *Kommentár a Büntető törvénykönyvhöz*. Budapest: CompLex.

Korinek, L. (2019) 'Drogok és emberek' in Bárd, P., Borbíró, A., Gönczöl, K. (eds.) *Kriminológia és kriminálpolitika a jogállam szolgálatában. Tanulmányok Lévay Miklós tiszteletére*. Budapest: ELTE Eötvös, pp. 175–186.

Krotoszynski, R. (2016) *Privacy Revisited. A Global Perspective on the Right to Be Left Alone*. Oxford: Oxford University Press; https://doi.org/10.1093/acprof:oso/9780199315215.001.0001.

Majtényi, L. (2006) *Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága.* Budapest: CompLex.

Menyhárd, A. (2014) 'A magánélethez való jog a szólás- és médiaszabadság tükrében' in Csehi, Z., Koltay, A., Navratyil, Z. (eds.) *A személyiség és a média a polgári és a büntetőjogban.* Budapest: Wolters Kluwer, pp. 177–226.

Navratyil, Z. (2014) 'Az ember névjogának kiterjesztő értelmezése mint a szólásszabadság lehetséges korlátja' in Csehi, Z., Koltay, A., Navratyil, Z. (eds.) *A személyiség és a média a polgári és a büntetőjogban.* Budapest: Wolters Kluwer, pp. 105–141.

Orwell, G. (1949) *Nineteen Eighty-Four.* London: Secker & Warburg.

Petrik, F. (ed.) (2017) *Az általános közigazgatási rendtartás magyarázata*. Budapest: HVG-Orac.

Péterfalvi, A., Révész, B., Buzás, P. (eds.) (2018) *Magyarázat a GDPR-ról.* Budapest: Wolters Kluwer.

Pokrócos, Gy. (2019) 'A rendőr képmásának nyilvánosságra hozatala', *Belügyi Szemle*, 67(2), pp. 89–108 [Online]. Available at: https://doi.org/10.38146/BSZ.2019.2.6 (Accessed: 10 October 2022).

Post, R. C. (1989) 'The Social Foundations of Privacy: Community and Self in the Common Law Tort', *California Law Review,* 77(5), pp. 957–1010 [Online]. Available at: https://doi.org/10.2307/3480641 (Accessed: 10 October 2022).

Prosser, W. L. (1960) 'Privacy', *California Law Review,* 48(3), pp. 383–423 [Online]. Available at: https://doi.org/10.2307/3478805 (Accessed: 10 October 2022).

Rubenfeld, J (1989) 'The Right of Privacy', *Harvard Law Review,* 102(4), pp. 737–807 [Online]. Available at: https://doi.org/10.2307/1341305 (Accessed: 10 October 2022).

Sándor, I. (2020) 'A képmáshoz való jog és a sérelemdíj bírósági gyakorlatának tendenciái', *Belügyi Szemle*, 68(4), pp. 53–69 [Online]. Available at: https://doi.org/10.38146/BSZ.2020.4.2 (Accessed: 10 October 2022).

Somody, B. (2016), 'A rendőrarcképmás-ügy mint az alapjogi ítélkezés próbája', *Fundamentum*, 20(1), pp. 103–112.

Sólyom, L. (1984) 'Polgárjog és polgári jog', *Jogtudományi Közlöny,*39(12), pp. 663–669.

Tóth, J. Z. (2017) 'Rendőrképmás: sajtószabadság és képmáshoz való jog a polgári jogi és az alapjogi jogosultságok keresztútján', *Pro Futuro*, 7(2), pp. 110–128 [Online]. Available at: https://doi.org/10.26521/Profuturo/2017/2/4766 (Accessed: 10 October 2022).

Warren, S., Brandeis, L. D. (1890) 'The Right to Privacy', *Harvard Law Review,* 4(5) pp. 193–220 [Online]. Available at: https://doi.org/10.2307/1321160 (Accessed: 10 October 2022).

Chapter IV

# Report on Privacy and Criminal Law in Croatia—Criminal Offenses Against Privacy in the Croatian Legal System

Marta Dragičević Prtenjača

## 1. Introduction

Technology is fabulous. It develops rapidly. Everything is available. In many ways, this is a good thought, but then again we are exposed. "Technology has transformed both the economy and social life."[1] Therefore, technology has also a dark side. Technology's gadgets (e.g., applications on smartphones for recording audio and video) are available to everyone. The possibility of easy recording and easy and fast storage of data, but also their transfer, increases the risk of invasion of privacy and violating the right to privacy. "The scale of the collection and sharing of personal data has increased significantly."[2]

Furthermore, when we are using various platforms, e.g., Facebook, Instagram, etc., or just searching something on Google, the providers are collecting data. All sorts of data are available including the one about us—personal data. Our personal data are available to almost everybody who is interested. "Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale to pursue their activities."[3] Various social networks on the web are

1 Recital 6 of the GDPR.
2 Recital 6 of the GDPR.
3 Recital 6 of the GDPR.

Marta Dragičević Prtenjača (2023) Report on Privacy and Criminal Law in Croatia—Criminal Offenses Against Privacy in the Croatian Legal System. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 111–163. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_4

providing more people with insight into the privacy of individuals. Therefore, the right to privacy of the individual is increasingly threatened in all its forms.

It is also the fact that individuals very often give their personal data voluntarily (on different social platforms), publicly, and globally, while there is also a movement to the protection of the right to privacy. It is called the "privacy paradox."[4] Where is the line?

Of course, when someone voluntarily gives his or her information, this is different from someone else collecting private information of the individual. Collecting the information of other individuals without their knowledge is spying. Connected to this is the problem of the publication of private data.

Those facts and developments suggest the need for stronger and more coherent data protection. Individuals should have guarantees and better control of their own personal data with better legal and practical certainty.[5]

Therefore, privacy and right to privacy must be protected at the international and national (constitutional and legislative) level because it forms a sort of the shield from intrusion of other people as well as the state and in that way protects the individuals and his/her rights. Its infringement must be prohibited and some sanctions must exist for its violation.

As *Archard* states, "the right to privacy serves principally as a constraint upon abuses of state power,"[6] but also from abuses of all other legal or physical persons. *Boban* states that privacy has absolute effect *erga omnes*; therefore, it has a vertical relationship toward state authorities, and a horizontal relationship toward everybody else.[7]

*Privacy, the right to privacy,* and *private space* are different terms that should not be understood as synonymous. *Privacy* is a term that each state defines in its own way (even each legal area has its own definitions). *The right to privacy* is the right of an individual to exercise privacy, and various international documents and national constitutions and laws protect it. *Private space* is a space "into which no one has the right to enter"[8] and in which the individual has the right to enjoy one's privacy. A private space is one "that no one has the right to enter,"[9] and any intrusion into that space could potentially constitute (among other violations) a violation of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 ("Convention").[10] It is understood quite broadly, because it is considered not only the home, but also the space outside the home, correspondence, but also other

4 For more see Kokolakis, 2017, pp. 122–134.
5 Recital 7 of the GDPR.
6 Archard, 2006, p. 14.
7 Boban, 2012, pp. 575–598.
8 Harris, O'Boyle and Warbric, 2009, p. 367.
9 Ibid.
10 The European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 [Online] Available at: https://www.echr.coe.int/documents/convention_eng.pdf (Accessed: 15 March 2022).

relationships, such as tapping telephone lines, which is an intrusion into an individual's private space. This understanding is based on the Anglo-Saxon principle that the individual has the right to keep for him- or herself everything one is and does, and even actions in public places can be considered private life, provided they are not harmful to society or the rights of others.

This privacy issue started in 19th century in the United States,[11] when judge Louis Brandeis and attorney Samuel Warren developed this notion which comprehends the right of an individual to be left alone. However, it must be noted, what they invented as *Glancy* notes is the *right* to privacy and not privacy itself.[12]

Unlike in Europe, where privacy is a guaranteed right of its citizens, in the US, "privacy" does not exist in the Constitution or Bill of Rights.[13] In one famous case *Griswold v. Connecticut* decision (381 U.S. 479) in the 1965 the Supreme Court found the right to privacy of the individual hidden in some provisions of the Constitution, especially the Fourth Amendment protection against search and seizure.[14] Hence, privacy is not explicitly stated in the Constitution, "it falls to Congress and the courts to determine the scope of that 'penumbra.'"[15]

Today, privacy is guaranteed with many international, regional, and national documents, e.g., the Universal Declaration of Human Rights (1948),[16] the Covenant on Civil and Political Rights (1966),[17] the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), the Declaration on Mass Communication Media and Human Rights ("Declaration on Mass Communication"),[18] the Charter of Fundamental Rights of the European Union,[19] the Treaty on the Functioning of the European Union (TFEU),[20] the Treaty on the European Union

11 Warren and Brandeis, 1890, p. 2.

12 Glancy, 1979, p. 1.

13 Information [Online] Available at: https://www.brookings.edu/blog/techtank/2018/07/05/suspected-criminals-get-privacy-rights-what-about-the-rest-of-us/#:~:text=In%20the%201965%20Griswold%20v,protection%20against%20search%20and%20seizure. (Accessed: 15 April 2022).

14 Ibid.

15 Ibid.

16 Universal Declaration of Human Rights 1948 (OG-MC-12/09) [Online] Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed: 17 February 2022).

17 Art. 17 of The International Covenant on Civil and Political Rights (1966) [Online] Available at: https://humanrights.gov.au/our-work/commission-general/international-covenant-civil-and-political-rights-human-rights-your (Accessed: 15 March 2022).

18 Council of Europe Declaration on Mass Communication media and Human Rights, Resolution 428 (1970) [Online] Available at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en. (Accessed: 15 March 2022).

19 Charter of Fundamental Rights of the European Union (2012/C 326/02) OJ C 326 [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN (Accessed: 30 March 2022).

20 Consolidated Version of The Treaty on the Functionign of the European Union OJ C 326/2012, 26.10.2012. [Online] Available at: http://data.europa.eu/eli/treaty/tfeu_2012/oj (Accessed: 30 March 2022) and [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN (Accessed: 30 March 2022).

(TEU),[21] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector,[22], the General Data Protection Regulation (GDPR),[23] etc.

In the Republic of Croatia, the right to privacy is guaranteed by the Constitution[24] and the provisions of ratified conventions, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms,[25] and European union legislative e.g., General Data Protection Regulation (GDPR),[26] and Implementation of the General Data Protection Regulation Act (IGDPRA).[27] Privacy is also protected by various national laws such as the Labor Act (LA),[28] Media Act

21 Treaty on the European Union, OJ C 326/2012, 26.10.2012. [Online] Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF (Accessed: 30 March 2022) and [Online] Available at: http://data.europa.eu/eli/treaty/teu_2012/oj (Accessed: 30 March 2022).

22 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002. [Online] Available at: http://data.europa.eu/eli/dir/2002/58/oj and at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 (Accessed: 15 March 2022).

23 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016. [Online] Available at: http://data.europa.eu/eli/reg/2016/679/oj and at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Accessed: 15 March 2022).

24 Constitution of the Republic of Croatia, Official Gazette, 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.

25 The European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 [Online] Available at: https://www.echr.coe.int/documents/convention_eng.pdf (Accessed: 15 March 2022).

26 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016 [Online] Available at: http://data.europa.eu/eli/reg/2016/679/oj and at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Accessed: 15 March 2022).

27 Implementation of the General Data Protection Regulation Act, Official Gazette, 42/18.

28 The Labor Act, Official Gazette, 93/14, 127/17, 98/19 provides in Art. 29 protection of the privacy of the employee.
(1) Personal data of employees may be collected, processed, used and delivered to third parties only if this is determined by this or another law or if it is necessary for the exercise of rights and obligations arising from employment, or in connection with employment.
(2) If the personal data referred to in para. 1 of this Art. need to be collected, processed, used or provided to third parties to exercise rights and obligations arising from the employment relationship, ie in connection with the employment relationship, the employer must determine in advance which data collect, process, use or deliver to third parties for this purpose.
(3) Personal data of employees may be collected, processed, used and delivered to third parties only by the employer or a person specifically authorized by the employer.
(4) Incorrectly recorded personal data must be corrected immediately.
(5) Personal data for the storage of which legal or factual reasons no longer exist must be deleted or otherwise removed.

(MA),[29] Electronic Media Act (EMA),[30] Consumer Protection Act (CPA),[31] Electronic Communications Act (ECA),[32] and of course if there is no adequate protection of this right, in other spheres of law, with the Penal Code (PC)[33] as "*ultima ratio*."

Hence, the primarily goal of this report is to provide an insight into the criminal law regulation of protection of privacy by stipulated criminal offences.

## 2. Privacy and the right to privacy in international and regional documents and in Croatia

The right to privacy is regulated in different international and regional documents. To this day, there is no generally accepted definition of privacy nor right to privacy. *Marmor* notes there are "differing views about the scope of the right and the kind of cases that fall under its purview."[34] Therefore, different documents but also countries define these notions in different ways, which vary depending on the context and circumstances prevailing in a particular society.

*Archard* defines privacy "as limited access to personal information."[35] By personal information, *Archard*[36] means someone's age, address, phone number, income, race, purchasing habits, ethnic origin, fingerprints, DNA, medical history, blood type, sexual orientation, religion, education, or political assimilation, etc., and by some decisions of the Court of Justice of the European Union (CURIA or CJEU or

(6) An employer who employs at least twenty workers is obliged to appoint a person who must enjoy the trust of the worker and who is authorized to supervise whether personal data are collected, processed, used and delivered to third parties in accordance with law.
(7) The employer, the person referred to in para. 6 of this Art. or another person who learns the personal data of the employee in the course of his / her duties, must keep these data permanently confidential.

29 The Media Act, Official Gazette, 59/04, 84/11, 81/13.

30 The Electronic Media Act, Official Gazette, 111/21.

31 The Consumer Protection Act, Official Gazette, 19/22.

32 The Electronic Communications Act, Official Gazette, 73/08, 90/11, 133/12, 80/13, 71/14, 72/17.

33 The Penal Code, Official Gazette, 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21.

34 Marmor, 2015, p. 1. at: https://d1wqtxts1xzle7.cloudfront.net/54794920/viewcontent-with-cover-page-v2.pdf?Expires=1652266275&Signature=KR3YwOgXHp-5Gc9rv9symxWbtn-C0umn33CFPMPX8y3NtTMZBecJ57kOowNDArHrehqUYKXJEHwSRYEvHeowbkhVnkxfgB1wDW4lpcc9HzHzK0nVHkAEoFHyZRdMTH-mKWzhejE7yiHmyGP0yBeuPawp0c-dt0eQPKnAqIvLy5hdPaQns5HbPY-pUBhdxp8nSwH9zZxq9zLYi90oqHhP3zFgzWDwyV67oinBltPHXQr3ZsMn8Ja46hjr-nOpLPunCm6AJklIgFaffXF37djRKYcP8w~w2MqLz-cVUwmCeuBPfiQV6kCVmNAr7ELOU2a-xPasQgUQ6zOeBrgxCFc2xA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (Accessed: 16 April 2022).

35 Moor (no date) cited in Archard, 2006, p. 16.

36 Ibid.

ECJ or Court of Justice)[37] even answers submitted by a candidate at a professional examination and any examiner's comments with respect to those answers constitute personal data, within the meaning of Art. 2(a) of Directive 95/46[38].

*Moor* defines the *right to privacy* as the "right to limit public access to oneself and to information about oneself."[39] Therefore, generally speaking, the right to privacy is the limitation of public access to information about someone.

The right to privacy has several forms: the right to a personal and family life, home, dignity, secrecy of correspondence and personal data, including photographs etc.

### *2.1. International documents*

The right to privacy is protected from encroachment by the state or other individuals and legal entities, by various fundamental international documents. Art. 12 of the Universal Declaration of Human Rights (1948) stipulates that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation" and that "everyone has the right to the protection of the law against such interference or attacks."[40]

Also, Art. 17 of the International Covenant on Civil and Political Rights (1966) also regulates this right,[41] which is identical in content to Art. 12 of the Universal Declaration of Human Rights.

### *2.2. Regional instruments*

#### *2.2.1. Documents of Council of Europe and European Court of human rights case law*

The and the Declaration on Mass Communication and the protection of the right to privacy and its implementation monitors the ECtHR with its case law.

37 Judgment of 20 December 2017, Nowak (C-434/16, EU:C:2017:994) at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8059397.

38 Court of Justice of the European Union, Fact sheet- Protection of personal data, p. 13. [Online] Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf (Accessed: 6 May 2022). See Judgment of 20 December 2017, Nowak (C-434/16, EU:C:2017:994), para. 62. [Online] Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8059397 (Accessed: 15 May 2022).

39 See Archard, 2006, p. 17.

40 Universal Declaration of Human Rights 1948 (OG-MC-12/09); [Online] Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed: 17 February 2022).

41 Art. 17. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; Everyone has the right to the protection of the law against such interference or attacks. the International Covenant on Civil and Political Rights (1966). [Online] Available at: https://humanrights.gov.au/our-work/commission-general/international-covenant-civil-and-political-rights-human-rights-your (Accessed: 15 March 2022).

Therefore, the Convention guarantees this right by Art. 8, according to which everyone is guaranteed the right to respect for his private and family life, home, and correspondence.

The following paragraph (2) prohibits public authority from interfering with or encroaching on the rights referred to in para. 1 unless such encroachment is necessary in a democratic society for the interests of national security, public order, economic welfare, prevention of disorder or crime, protection of health or morals or rights, and freedom of others.[42] This is an exclusion clause with content of the restriction of certain fundamental rights and freedoms. Provision speaks of the possibility of government interference to restrict certain human rights to protect certain legitimate interests.

The provision of Art. 17 of the Convention prohibits the abuse of rights in the sense that nothing stated in the Convention may be interpreted as destroying or restricting the rights and freedoms recognized by the Convention largely than provided for in the Convention.

The ECtHR has also decided the scope of the right to privacy, which in *Niemietz v. Germany (1992)*[43] took a position on the concept of private life: that private life does not include only the so-called "inner circle" of an individual, but also other connections with the environment and relationships with other people.[44] This is because private life includes the freedom to establish connections with others, and which is a social continuation of the fundamental inner circle of the individual. In *McFeeley v. The United Kingdom* (1980), the Commission emphasized the importance of relationships and connections with other people, concluding that prisoners also have the right to privacy and need to be given some degree of relationship with others.[45]

The Court has held that surveillance of persons in public places by the use of photographic means does not, as a rule, constitute an invasion of an individual's privacy and interference with his or her private life, but recording, storing or using such information may violate Art. 8 of the Convention.[46] Therefore, the Court wanted to make a distinction "between the monitoring of an individual's acts in a public place for security purposes and the recording of those acts for other purposes, going beyond what the person could possibly have foreseen"[47] to establish the strict boundary of private life as guaranteed under Art. 8. In *Peck v. the United Kingdom,*[48] there was

42 Art. 8, para. 2 of the Convention.

43 ESLJP case of *Niemietz v. Germany* (Appl. no. 13710/88), 16 December 1992. [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22NIEMIETZ%20v.%20GERMANY\%22%22],%22itemid%22:[%22001-57887%22]} (Accessed: 15 March 2022).

44 Harris, O'Boyle and Warbric, 2009, p. 364.

45 Harris, O'Boyle and Warbric, 2009, p. 364.

46 Harris, O'Boyle and Warbric, 2009, p. 265.

47 Guide to the case law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 33.

48 ESLJP case *Peck v. the United Kingdom* (App.no. 44647/98), 28 January 2003 (28.04.2003), §§59–62. [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Peck%20v.%20the%20United%20Kingdom%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-60898%22]} (Accessed: 15 May 2022).

a violation of Art. 8, even though the plaintiff had attempted to commit suicide by cutting his wrists in public place and was recorded by street surveillance camera, of which he was not aware at the time.[49]

In ECtHR case law, personal data is defined as:

> any information relating to an identified or identifiable individual….such data cover not only information directly identifying an individual (the "data subject"), such as surname and forename (Guillot v. France, 1996, §§21-22; Mentzen v. Latvia (dec.), 2004; Güzel Erdagöz v. Turkey, 2008, §43; Garnaga v. Ukraine, 2013, §36; Henry Kismoun v. France, 2013, §25; Hájovský v. Slovakia, 2021 §§11-12 and 41), but also any element indirectly identifying a person such as a dynamic IP (Internet Protocol) address (Benedik v. Slovenia, 2018, §§107-108).[50]

Personal data by ECtHR case law can take different forms, e.g., cellular samples and DNA profiles or fingerprints; data on the birth and abandonment of an individual, including information needed to discover the truth about an important aspect of personal identity; Internet subscriber information and specific IP addresses; recordings as voice samples; information on banking documents, data on Internet and messaging usage by an employee in the workplace, obtained through surveillance; electronic data seized in a law firm, even though it had not been deciphered, transcribed, or officially attributed to their owners; data collected in the context of non-covert video surveillance in a university; information on the taxable income and assets of a large number of individuals etc.[51]

49 Afterward, one Media House used a photograph of the incident involving the applicant on its front page to accompany an article on the use and benefits of the CCTV system and the applicant's face was not specifically masked—Case *Peck v. the United Kingdom,* paras. 9–14.

50 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on December 31, 2021), p. 7. Also see *Amann v. Switzerland* [GC], 2000, Art. 65; *Haralambie v. Romania,* 2009, para. 77.

51 Guide to the Case law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 7. also see *Amann v. Switzerland* [GC], 2000, para. 65; *Haralambie v. Romania,* 2009, Para. 77. Personal data can take very different forms. For example:
- Internet subscriber information associated with specific dynamic IP addresses assigned at certain times (Benedik v. Slovenia, 2018, paras. 108–109).
- Recordings taken for use as voice samples, being of a permanent nature and subject to a process of analysis directly relevant to identifying a person in the context of other personal data (P.G. and J.H. v. the United Kingdom, 2001, para. 59).
- Cellular samples and DNA profiles (S. and Marper v. the United Kingdom [GC], 2008, paras. 70–77) or finger prints (Ibid., para. 84) which, notwithstanding their objective and irrefutable character, contained unique information on the individual concerned and allowed his/her precise identification in a wide range of circumstances (Ibid., para. 85).
- Information on a given individual obtained from banking documents, whether involving sensitive details or professional activity (M.N. and Others v. San Marino, 2015, paras. 51 *et seq.*).
- Data on the occupation of an identified or identifiable individual collected and stored by the police (Khelili v. Switzerland, 2011, para. 56).

ECtHR assures protection as regards Art. 8 (right to respect for their private life), not only to a physical person, individuals, but also the legal persons and entities (*Société Colas Est and Others v. France),*[52] if they are directly affected by a measure that breaches their right to respect for their "correspondence" or "home," e.g.: where a company had been ordered to provide a copy of all data on a server shared with other companies[53] or where the Ministry of Defense, under a warrant, had intercepted the communications of civil liberties NGOs (*Liberty and Others v. the United Kingdom,* 2008, paras. 56–57).[54]

Hence, it must be noted how for Art. 8 to be applied the personal data and its processing must have a certain level of seriousness and in a manner causing prejudice to personal enjoyment of the right to respect for private life.[55] In one case where Croatia was involved (*Vučina v. Croatia*)[56] within this context, the ECtHR rejected as incompatible *ratione materiae* a complaint about the publication of a photograph in a women's magazine *Gloria*, under an erroneous title which had referred to the applicant

– Data on Internet and messaging (Yahoo) usage by an employee in the workplace, obtained through surveillance (Bărbulescu v. Romania [GC], 2017, paras. 18, 74–81).
– A copy of electronic data seized in a law firm, even though it had not been deciphered, transcribed or officially attributed to their owners (Kırdök and Others v. Turkey, 2019, para. 36).
– Data collected in the context of non-covert video surveillance in a university (Antović and Mirković v. Montenegro, 2017, paras. 44–45).
– Information on the taxable income and assets of a large number of individuals, notwithstanding the fact that the public could access such data under certain conditions (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], 2017, para. 138).
– Data on the birth and abandonment of an individual, including information needed to discover the truth about an important aspect of personal identity (Gaskin v. the United Kingdom, 1989, Art. 39; Mikulić v. Croatia, 2002, Arts. 54-64; Odièvre v. France [GC], 2003, paras. 28–29).
– Data included in a divorce settlement, comprising details as to the division of matrimonial assets, the custody and residence of minor children, the alimony agreement, and an overview of the assets/income of the applicant (Liebscher v. Austria, 2021, paras. 31 and 68). Guide to the Case law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 8.

52 See Judgment ECtHR, *Société Colas Est and Others v. France*, (Appl. no. 37971/97), 16th April 2002 (final 16/07/2002), para. 40; [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Soci%C3%A9t%C3%A9%20Colas%20Est%20and%20Others%20v.%20France%20,%22],%22itemid%22:[%22001-60431%22]} (Accessed: 28 March 2022).

53 Bernh Larsen Holding AS and Others v. Norway, 2013, para. 106.

54 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 8. It was diferrnet in a case concerning measures involving the protection of personal data of members of a religious organisation and respect for their "private life," the organisation was not directly affected, and was thus not a "victim" within the meaning of Art. 34 of the Convention (Avilkina and Others v. Russia, 2013, para. 59).—Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 8. See also *M.L. and W.W. v. Germany*, 2018, para. 88.

55 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 11.

56 For more see Judgement ECtHR *Vučina v. Croatia* (Appl. no. 58955/13), 31 October 2019. para. 50. [Online] Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-198384%22]} (Accessed: 29 March 2022).

as someone else. In the Court's view, the low degree of seriousness of that error and the very limit inconvenience caused was not sufficient for Art. 8 to be engaged.[57]

ECHR and ECtHR allow in some situation and under strict conditions an interference with the right in Art. 8 of the Convention.[58] It is so called the "three-part test." It is fulfilled if an interference:

(1) Is "in accordance with the law";
(2) Must pursue a "legitimate aim"; and
(3) Must be "necessary in a democratic society."[59]

In the Declaration on Mass Communication,[60] the right to privacy is defined as "the right to live one's life with minimal interference" by others.[61] This right includes private, family, and domestic life, psychological and moral integrity, honor and reputation, protection against defamation, non-disclosure of irrelevant and unpleasant facts, protection against publishing private photographs without consent, and protection against publishing information given or received in confidence.[62] The Declaration on Mass Communication notes how protection of the Art. 8 of the Convention extends not only to an individual against interference by public authorities, but also against interference by private persons or institutions, including the mass media, so "national legislations should comprise provisions guaranteeing this protection."[63] In Croatia this issue is regulated with the Media Act (MA), the Electronic Media Act (EMA), the Electronic Communications Act (ECA), and the Consumer Protection Act (CPA).

It also elaborates on issues and dangers like problems that arise for the persons in public life. "The phrase "where public life begins, private life ends" is inadequate to cover this situation."[64] It is explicitly stated that: private lives of public figures are entitled to protection, save where they may have an impact upon public events and the fact that an individual figure in the news does not deprive him of a right to a private life.[65]

The Declaration on Mass Communication also recognizes the problem of obtaining the information "by modern technical devices (wiretapping, hidden microphones, the

57 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on December 31, 2021), p. 11.

58 "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." (Art. 8, para. 2).

59 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 24.

60 Council of Europe Declaration on Mass Communication Media and Human Rights, Resolution 428 (1970), [Online] Available at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en. (Accessed: 15 March 2022).

61 Art. 16 of the Declaration on Mass Communication.

62 Art. 16 of the Declaration on Mass Communication.

63 Art. 21 of the Declaration on Mass Communication.

64 Art. 17 of the Declaration on Mass Communication.

65 Art. 17 of the Declaration on Mass Communication.

use of computers, etc.), which infringe the right to privacy"; it concludes, "Further consideration of this problem is required."[66]

### *2.2.2. The European Union*

The Charter of Fundamental Rights of the European Union[67] regulates right to privacy in its Art. 7 (respect for private and family life), Art. 8, (protection of personal data), Art. 9 (right to marry and start a family) and Art. 10 (freedom of thought, conscience, and faith), while the TFEU[68] in its Art. 16 states how "everyone has the right to the protection of personal data concerning them."[69]

The TEU[70] in its Art. 39 states that all Member States stats will have to make "rules relating to the protection of individuals with regard to the processing of personal data"[71] which was the basis for today's GDPR.[72]

European Union Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, which was passed in 2002,[73] also refers to privacy through private life and restricts collecting of that data, so it notes that the data relating to subscribers,

66 Art. 18 of the Declaration on Mass Communication.

67 Charter of Fundamental Rights of the European Union (2012/C 326/02) OJ C 326; [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN (Accessed: 30 March 2022).

68 Consolidated Vesrion of the Treaty on the Functionign of the European Union OJ C 326/2012, 26.10.2012.; [Online] Available at: http://data.europa.eu/eli/treaty/tfeu_2012/oj (Accessed: 30 March 2022) and [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN (Accessed: 30 March 2022).

69 Art. 16, para. 1 of the TFEU.

70 Treaty on the European Union, OJ C 326/2012, 26.10.2012. [Online] Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF (30.03.2022.) and at: http://data.europa.eu/eli/treaty/teu_2012/oj (Accessed: 30 March 2022).

71 Art. 39 of TEU: "In accordance with Art. 16 of the Treaty on the Functioning of the European Union and by way of derogation from para. 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

72 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016. [Online] Available at: http://data.europa.eu/eli/reg/2016/679/oj and at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Accessed: 15 March 2022).

73 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002. [Online] Available at: http://data.europa.eu/eli/dir/2002/58/oj and [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 (Accessed: 15 March 2022).

processed in electronic communications networks to establish connections and transmit information, contain information on the private life of natural persons. Legal persons have a right to the privacy their correspondence or their legitimate interests. Such data may only be stored to the extent that is necessary for the provision of the service for billing and for interconnection payments, and for a limited time.[74]

It also prohibits further processing of data that the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value-added services,[75] unless the subscriber has agreed to this based on accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing.[76]

Today, the GDPR explicitly notes how this regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system,[77] and respects all fundamental rights and observes the freedoms and principles recognized in the charter as enshrined in the treaties, in particular the respect for private and family life, home, and communications, the protection of personal data, freedom of thought, conscience, and faith, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious, and linguistic diversity.[78]

### *2.2.3. Regional documents in the world*

In 1990, the UK Committee on Privacy and Related Issues adopted a definition of privacy as "the right of an individual to be protected from intrusion into his or her private life and affairs, or the life and affairs of his or her family, by physical means or disclosure."[79] The Human Rights Act 1998 incorporates the rights set out in the ECHR into domestic British law, and guarantees them to

74 Para. 26 of the Directive 2002/58/EC.
75 Para. 26 of the Directive 2002/58/EC.
76 Para. 26 of the Directive 2002/58/EC.
77 Art. 2, para. 1 of the GDPR.
78 Recital 4 of the GDPR.
79 Report of the Committee on Privacy and Related Matters; Chairman, 1990, cited in Marshall, 2009 and cited in Maralayn, 2012, p. 5. [Online] Available at: https://law.aua.am/files/2012/03/PAPER.pdf (Accessed: 15 April 2022). For comparation of the Protection of Private Life of Public Officials and Public Figures Guaranteed by the Constitution of the United States and European Convention for the Protection of Human Rights and Fundamental Freedoms, see Maralyan, 2012, pp. 20–24.

every citizen in the UK.[80] The Data Protection Act 2018 is the UK's implementation of the GDPR.[81]

Right of privacy is, "in US law, an amalgam of principles embodied in the federal Constitution or recognized by courts or law-making bodies concerning what Louis Brandeis, citing Judge Thomas Cooley, described in an 1890 paper (co-written with Samuel D. Warren) as 'the right to be let alone.'"[82] Therefore, in the literature, *Warren and Brandeis* was the first case to use that term.[83]

The Australian Privacy Charter (1994)[84] defines this right as "the autonomy of the individual and as a restriction on the right of the state and private organizations to encroach on that autonomy" which is guaranteed in a free and democratic society. This term includes the right of an individual to the privacy of his or her body, private space, privacy of communications, personal data, and the right to freedom of control.[85]

### *2.3. Legislative situation in Croatia*

In Croatia, as it was mentioned before, there is no unique definition of privacy or right to privacy. The right to privacy is guaranteed by the Constitution of the Republic of Croatia in various provisions, but also in the aforementioned regulations. Protection of various rights and freedoms is regulated in Art. 14 of the Constitution, which states that everyone in the Republic of Croatia, regardless of their social origin, sex, race, religion, and other characteristics has rights and freedoms, and all are equal before the law.

Furthermore, those rights and freedoms are not absolute. The Croation Constitution in Art. 16 allows the possibility of some restrictions of the guaranteed rights and freedoms: only laws may restrict the rights and freedoms of citizens to protect the freedoms and rights of others, the rule of law, public morals, and health, and any

80 The Human Rights Act came into force in the UK in October 2000. [Online] Available at: https://www.equalityhumanrights.com/en/human-rights/human-rights-act#:~:text=The%20Human%20Rights%20Act%201998%20sets%20out%20the%20fundamental%20rights,the%20UK%20in%20October%202000. (Accessed: 2 April 2022).

81 The Data Protection Act 2018 [Online] Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Accessed: 30 March 2022). More information [Online] Available at: https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK's%20implementation%20of,used%20fairly%2C%20lawfully%20and%20transparently (Accessed: 30 March 2022).

82 Encyclopaedia Britannica [Online] Available at: https://www.britannica.com/topic/rights-of-privacy (Accessed: 11 March 2022).

83 See Warren and Brandeis, 1890, p. 205.

84 Australian Privacy Charter (1994) [Online] Available at: https://www.privacy.org.au/About/PrivacyCharter.html (Accessed: 15 February 2022).

85 Australian Privacy Charter (1994) "A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy." "People have a right to the privacy of their own body, private space, privacy of communications, information privacy (rights concerning information about a person), and freedom from surveillance.."

restriction of these rights and freedoms must be proportionate to the nature of the need for restriction in each case.

Therefore, any encroachment on the rights and freedoms of other people must be justified from the aspect of Art. 16 of the Constitution, the right to privacy also among other rights.

The right to privacy, as it was stated before, takes several forms and different constitutional provisions guarantee its protection, e.g., Art. 34 guarantees the inviolability of the home, as a form of privacy. Art. 35 guarantees everyone the right to personal and family life, dignity, honor, and reputation, while Art. 36 prescribes the freedom and secrecy of correspondence and all other forms of communication. Art. 37 guarantees the security and confidentiality of personal data, and Art. 40 the right to religion and religious beliefs. All the above articles of the Constitution guarantee various forms of privacy and point to the need to protect them by law. Interpretation of the above provisions of the Convention and the Constitution of the Republic of Croatia leads to the interpretation that no one (government or other persons) may take actions that would limit the rights of others as provided by the relevant provisions of these documents.

The GDPR has direct application,[86] and it is (also) stated by Implementation of the General Data Protection Regulation Act (IGDPRA). Therefore, it is part of the internal legal order. IGDPRA specifically regulates the founding of the Croatian Personal Data Protection Agency,[87] its powers and everything related to Agency.[88] It also regulates the National Accreditation Body, personal data processing in special cases (especially when child is in question), etc. The Agency is in charge for monitoring of the application of the GDPR, headed by the director of the agency.[89] By GDPR provisions everyone who collects the data ("collectors" or "processors")[90] must appoint a data protection officer.[91] Anyone who considers that a right guaranteed by GDPR has been violated, can lodge a complaint and may submit a request to the Agency for rights violation.[92] The Agency submits an annual report on the work of the personal data protection agency to the Croatian Parliament.[93]

86 "Consequently, on April 27, 2018, the Republic of Croatia adopted the Act on the implementation of the General Data Protection Regulation which entered into force on 25 May 2018 (OG 42/18)" and the Agency as a supervisory body is founded by that Act—information available at [Online] Available at: https://azop.hr/rights-of-individuals/ (Accessed: 28 March 2022).

87 For more information see [Online] Available at: https://azop.hr/naslovna-english/ (Accessed: 15 March 2022).

88 See Arts. 6–18 of the IGDPRA.

89 For more information see [Online] Available at: https://azop.hr/organizacijska-struktura/ (Accessed: 15 March 2022).

90 Art. 4 dots. 7 and 8 of the GDPR.

91 Arts. 13, 14 and 30 of the GDPR.

92 For more information see [Online] Available at: https://azop.hr/rights-of-individuals (Accessed: 15 March 2022).

93 Annual report on the work of the personal data protection agency for the period from 1 January 2020 to 31 December 2020. [Online] Available at: https://www.sabor.hr/sites/default/files/uploads/sabor/2021-04-01/134202/GODISNJE_IZVJESCE_AZOP_2020.pdf (Accessed: 20 March 2022), also see Art. 17 of the IGDPRA.

The MA defines privacy as family and personal life and right to live by one's own choice.[94] Its Art. 7 regulates the right to privacy of everyone,[95] even a person performing public service or duty "except in cases related to public service or duty performed by a person."[96] This is in line with the case law of the European Court of Human Rights, which provides protection to public and "relatively" public figures from invading their privacy, if the recordings made are not related to the function they perform. The legislature distanced himself from special cases when a person attracts public attention with his statements, behavior, and other acts from personal or family life, so he prescribed that in such cases these persons cannot "demand the same level of privacy as other citizens."[97] Also, the MA provides the situation when there is no violation of the right to privacy if, in terms of information, a legitimate public interest prevails over the protection of privacy in relation to the activity of journalists or information.[98]

The Electronic Media Act forbids publication of information that reveals the identity of a child under the age of 18 involved in cases of any form of violence, regardless of whether the witness, victim, or perpetrator or the child attempted or committed suicide, nor disclose details of the child's family relationships and private life,[99] and the personal data of minors collected or otherwise obtained by media service providers within the framework of technical measures for the protection of minors may not be processed for commercial purposes, such as direct marketing, profiling, and targeted behavioral advertising.[100]

The Consumer Protection Act explicitly forbids the merchant the transfer of personal data to any third person contrary to the GDPR[101] and obliges the merchant of data processing in accordance with GDPR (Art. 83, para. 5 and 6) while the Electronic Communications Act protects the privacy and personal data explicitly in its Arts. 5 and 42, (para. 1), 43, 44, and 99a.

If none of this is enough to protect the privacy, then comes the criminal law with its regulations. The criminal law names several crimes against privacy in the chapter "Criminal Offences against Privacy"—e.g., Violation of the Inviolability of the Home

94 Art. 2 of the MA.
95 Art. 7, para. 1 of the MA.
96 Art. 7, para. 2 of the MA.
97 Art. 7, para. 3 of the MA.
98 Art. 8 of the MA.
99 Art. 24, para. 5 of the EMA. "(5) It is not allowed to publish information revealing the identity of a child under the age of 18 involved in cases of any form of violence, regardless of whether the witness, victim or perpetrator or the child attempted or committed suicide, nor disclose details of the child's family relationships. and private life."
100 Art. 24, para. 6 of the EMA. "(6) Personal data of minors collected or otherwise obtained by media service providers within the framework of technical measures for the protection of minors may not be processed for commercial purposes, such as direct marketing, profiling and targeted behavioral advertising."
101 Art. 11 of the GDPR. It also regulates the protection of personal data in cases of determination of the contract (Art. 83).

and Business Premises[102]; Violation of the Secrecy of Letters and Other Parcels[103]; Unauthorized Audio Recording and Eavesdropping[104]; Unauthorized Taking of Pictures[105]; Abuse of Sexually Explicit Footage[106]; Unauthorized Disclosure of a Professional Secret[107] and Unlawful Use of Personal Data[108].

Some criminal offences against privacy can be found in other chapters, as criminal offences against Marriage, Family, and Children (Violation of the Privacy of the Child; in Art. 178 PC), but also in chapter regulating criminal offences against judiciary (Disclosing the Identity of a Person at Risk or Protected Witness; in Art. 308 PC).

## 3. Criminal regulation of the right to privacy in the Republic of Croatia

Privacy in Croatia is protected, as was already mentioned, through a variety of different laws. When there is no adequate protection accomplished by other branches of law, then the protection of right to privacy is guaranteed and given by criminal law (as *ultima ratio).*

In 2011, Croatia got the a Penal Code, with new chapter "Criminal Offences against Privacy." The object of protection is privacy, which, as stated, is not unanimously defined, but the private sphere of individuals includes the physical and mental interests of individuals, their sexual life, gender, and sexual orientation, personal data, reputation, and photographs.[109]

Most of the criminal offences against privacy are in the special chapter entitled "Criminal Offences against Privacy." Some other offences which can be found in other chapters of the Croatian Penal Code are also offences against privacy and they are protecting more than one legal good (e.g., privacy and child, etc.). Hence, Violation of the Privacy of the Child[110] is in the chapter "Criminal offences against Marriage, Family, and Children," and the Disclosing the Identity of a Person at Risk or Protected Witness[111] is in the chapter "Criminal Offences against the Judiciary."

102 Art. 141 of the Penal Code.
103 Art. 142 of the Penal Code.
104 Art 143. of the Penal Code.
105 Art. 144. of the Penal Code.
106 Art. 144a of the Penal Code.
107 Art. 145. of the Penal Code.
108 Art. 146. of the Penal Code.
109 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, pp. 159–160; see also *Niemietz v Germany.*
110 Art. 178 of the Penal Code.
111 Art. 308 of the Penal Code.

### *3.1. Violation of the inviolability of the home and business premises*

Violation of the Inviolability of the Home and Business Premises[112] protects the privacy in home or in the business premises. A perpetrator is anyone who enters without authorization another person's home or business premises, or a closed or enclosed space belonging to the home or business premises, or who does not leave when requested to do so by the authorized person.[113]

Entering without authorization means any entry, despite the explicit opposition of an authorized person, and not leaving upon request means refusal to leave the dwelling. Therefore, this criminal offence can be committed by both act and omission.[114]

The act can be committed by anyone (the so-called *delictum communium*), but if it is committed by an official in the performance of service or a responsible person in the exercise of public authority, it will be a more serious, qualified form: aggravated offence. Criminal offence from para. 1 will be prosecuted upon request,[115] and stipulated punishment is imprisonment for a term of up to one year.[116]

An aggravated form of the offence violates not only one's privacy, but also the trust that citizens have in institutions and the lawful and effective exercise of public authority.[117] For aggravated forms, the person can be sentenced to imprisonment for a term not exceeding three years.[118]

Croatian legislature decided to protect the privacy of the business premises as well, although Art. 8 of the ECHR does not specifically mention business premises.[119] The reason lies in ECtHR case law, which interpreted the notion of home dynamically and extensively, in such a way that it extended protection to those premises as well, i.e., premises used by an individual to earn a living.[120]

In case of the ECHR's *Société Colas Est and Others v. France*,[121] the Court stated that even the right of a legal person to respect its registered office, branch, and other business premises might fall under the protection of Art. 8 of the ECHR. Art. 34 of the (Croatian) Constitution also does not mentions premises. It speaks only of the inviolability of the home, but the term can be stretched to include premises in which the addressees perform activities more permanently, such as business premises used

112 Art. 141 of the Penal Code.
113 Art. 141, para. 1 of the Penal Code.
114 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 164.
115 Art. 141, para. 3 of the Penal Code.
116 Ibid.
117 Art. 141, para. 2 of the Penal Code If the criminal offence referred to in para. 1 of this Art. is committed by an official person in exercising its official duty, or public official in the exercise of public authority, he/she shall be sentenced to imprisonment for a term of up to three years.
118 Art. 141, para. 2 of the Penal Code.
119 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, pp. 165–166.
120 See ECtHR, *Niemietz v. Germany*, 1992, paras. 29–33.
121 See ECtHR, *Société Colas Est and Others v. France*, 2002, para. 40.

based on property or a legal basis.[122] Croatian doctrine and literature has taken the standpoint about notion of home, which should be interpreted extensively and expended to all spaces used in the function of home even if there are different spaces, which do not have to be real estate. Therefore, by this interpretation, a home does not represent only the usual spaces for residence, e.g., houses, apartments, and cottages, but subtenant rooms, mobile homes, residential caravans, ship cabins, and even tents can also be considered as a home.[123] The legal text extends the protection to closed or fenced areas that belong to the home. These are spaces such as woodsheds, laundries, pantries, basements, yards, gardens, toilets, warehouses, basements, attics, etc.[124]

However, it is debatable whether an uninhabited apartment can be considered a home in the sense of this incrimination in our criminal law theory and case law. According to the Apartment Rental Act (APA),[125] an apartment is a set of rooms intended for housing with much-needed ancillary rooms that form a single closed building unit and have a separate entrance.[126]

The concept of "home" is in one sense broader than the concept of "apartment," because it includes spaces that do not necessarily form a closed building unit; on the other hand, if we look to the functional definition of home, the concept of apartment can be considered more broadly. The reason for this is that the premises—which do not yet have the function of home, although they are intended for that function—are excluded from the notion of "home," but not "apartment."[127] Therefore, *Munivrana Vajda* considers that given the diverse nature of the space whose inviolability is protected by this incrimination, obviously their functional feature, the fact that they are used as a home, is essential. Such a conclusion, after all, is in line with the functional–subjective definition of the notion of home in criminal procedural law. Perhaps the most important argument in favor of a functional interpretation rests on a systematic–teleological interpretation of this norm, based on the protective object and the whole in which it is included, especially since January 1, 2013. According to the new Criminal Code, the group legal good that is protected by this chapter, and thus by this criminal offense, is privacy, and when it comes to an uninhabited, empty apartment, the private domain of an individual is not violated.[128]

It can be also concluded how deciding upon the question whether something is home must be *quaestio facti* in each case. The mere fact that the tenant is absent from the home even for a long time does not deprive the space of protection from

122 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p 161.
123 Ibid.
124 Ibid.
125 The Apartment Rental Act, OG, 91/96, 48/98, 66/98, 22/06, 68/18, 105/20.
126 Art. 2, para. 1 of APA.
127 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 162.
128 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 163.

the inviolability of privacy. Therefore, the spaces that an individual only periodically uses are also to be considered as home (e.g., holiday homes).[129]

An authorized person is not necessarily the owner. It can also be a tenant, even in a relationship with the property owner, i.e., the owner of the apartment.[130] However, the person who has illegally occupied someone else's apartment does not enjoy protection of this Article.[131]

Business premises are according to the Lease and Sale of Business Premises Act (LSBPA),[132] "an office building, business premises in narrow sense, garage and garage space."[133] Business premises in a narrow sense are "one or more premises in a business or residential building intended for the performance of business activities which, as a rule, form an independent usable unit and have a separate main entrance."[134] The business building is considered "a building intended for the performance of business activities if it is mostly used for that purpose."[135]

In Croatian criminal law case law, there was one interesting case. A neighbor rang the doorbell of a neighbor who lived immediately above to warn her of leaking water from her apartment. When he entered, he asked for a glass of water. The neighbor gave him the water. Then he grabbed her and dragged her to the bedroom. She begged him to stop and leave the apartment, which he refused to do. She started screaming than he ran out of the apartment and threatened to kill her if she reported it to the police. He was charged for Violation of the Inviolability of the Home and Business Premises[136] and Threat[137], and was convicted for both offences, for concurrence of offences and sentenced to seven months of suspended sentence with probation period of three years.[138] He was of diminished responsibility due to some psychiatric problems, which influenced the sentence.

In case *Khan v. the United Kingdom*[139] the ECtHR found a violation of Art. 8, although the applicant was not in his own apartment but in the home of the third person (who was also not aware of the surveillance), whom he had visited and in spontaneous conversation admitted he participated in a drug-related case—he was a drug dealer.

129 Ibid. p. 163.
130 Ibid. p. 64.
131 Ibid. p. 164.
132 The Law on Lease and Sale of Business Premises, Official Gazette, 125/11, 64/15, 112/18.
133 Art. 2, para. 2 of LSBPA.
134 Art. 2, para. 4 of LSBPA.
135 Art. 2, para. 3 of LSBPA.
136 Art. 141, para. 1 of the Penal Code.
137 Art. 139, para. 2 of the Penal Code.
138 Dicision of the Municipal Criminal Court in Zagreb, no. K-129/19.
139 ECtHR case *Khan v. the United Kingdom* (Appl. no. 35394/97), May 12, 2000 (final 04.10.2000.), §§25–28. [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Khan%20v.%20the%20United%20Kingdom%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58841%22]} (Accessed: May 15, 2022).

### *3.2. Violation of the secrecy of letters and other parcels*

The Violation of the Secrecy of Letters and Other Parcels,[140] also protects the right to privacy. Written correspondence often contains private information that are intimate, personal, or deal with family life, etc. Such correspondence is private and in that context is considered secret. This does not mean that the information contained in that correspondence must be kept secret or classified as secret. The content of the correspondence must remain available only to the intended recipient. The secrecy in this crime comprehends this context. The protection of this secrecy is a prerequisite for free and secure communication, and its importance is guaranteed in a number of international documents.[141] The right to correspondence and privacy in correspondence is guaranteed by the Universal Declaration of Human Rights[142] and the European Convention for the Protection of Human Rights[143], and is also guaranteed by the Constitution of the Republic of Croatia (Art. 36—The right to secrecy of letters and consignments)[144]

Criminal protection of letters and other parcels can be divided into two main directions. As *Grozdanić* points out, it can consist in (a) protecting the secrecy of the content whoever opens without authorization another person's parcel, letter, telegram, electronic mail or any other item of correspondence or otherwise violates his or her secrecy, [145] or (b) protecting the written communication[146] of persons from any who, without authorization, retain, conceal, destroy, or hand over without authorization to a third party another person's sealed parcel or letter, telegram, electronic mail, or any other item of correspondence.[147]

The object of the action is a closed letter, parcels, telegram, e-mail or any other means of correspondence and the action on that object must be undertaken by a person who is not the addressee or is not intended for him.[148]

The *modus operandi* includes three modes:

a) opening;

b) breach of secrecy in another way; and

c) retaining, concealing, destroying, or handing it over to another.[149]

140 Art. 142 of the Penal Code.

141 For more see Bojanić et al., 2011, p. 72.

142 Art. 12. See Universal Declaration of Human Rights [Online] Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed: 23.03.2022.).

143 Art. 8, para. 1. See European Convention for the Protection of Human Rights and Fundamental Freedoms p. 11. [Online] Available at: https://www.echr.coe.int/documents/convention_eng.pdf (Accessed: March 23, 2022).

144 Art. 36 of the Constitution of the Republic of Croatia "Freedom and secrecy of correspondence and all other forms of communication are guaranteed and inviolable. Only the law may prescribe restrictions necessary for the protection of security or the conduct of criminal proceedings."

145 Art. 142, para. 1 of the Penal Code.

146 Bojanić et al., 2011, p. 72.

147 Art. 142, para. 1 of the Penal Code.

148 For more see Bojanić et al., 2011, pp. 72–73.

149 Bojanić et al., 2011, p. 72.

Opening would mean any mechanical removal of obstacles to the contents of the letter, while the other way would include any way by which someone acquainted with the contents of letters, shipments, etc., without opening them, i.e., using existing scientific technology (e.g., infrared radiation, etc.).[150] The third mode encompasses the ways in which the object of action seems inaccessible to the addressee.

Each of the actions must be unauthorized, i.e., without the authorization of the person for whom it is intended or without a legal basis. The legal basis is the reason for excluding unlawfulness. For example, the investigating judge may order the detention and delivery of letters, telegrams and parcels intended for the defendant in accordance with Art. 339 of the Criminal Procedure Act (CPA).[151] In that case, a criminal offense will not be committed because it is not unlawful.

For the basic form of the offence, the stipulated punishment is imprisonment for a term of up to one year, or in other words, a fine or custodial sentence from three months to one year.

The aggravated form of the offence is when someone wants to buy others' information or to damage someone with information from the letters, parcels, or telegrams (etc.), or when someone, acting with the aim of acquiring pecuniary gain for himself/herself or another or of causing damage to another, discloses to a third party a piece of information that he/she came to know by violating the secrecy of another person's parcel, letter, telegram, electronic mail, or any other item of correspondence, or makes use of this secret.[152]

In addition, for that form, the perpetrator can be punished with fine or imprisonment for a term of up to two years. For both forms of this criminal offence, the prosecution will begin upon request.[153]

The most severe form of the offence is when either of the previous forms are committed by an official person in exercising its official duty or by a public official in the exercise of public authority, and such perpetrator can be punished with fine or imprisonment up to three years.[154]

In Croatia, there were cases where the mail carrier opened the msil of senior citizens and stole their pensions.[155] Another case which was prosecuted on the Zagreb Municipal Court was when ex-husband looked at e-mail of his ex-spouse. He was acquitted because of the lack of evidence.[156]

150 Ibid.

151 The Criminal Procedure Act, Official Gazette, 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 126/19.

152 Art. 142, para. 2 of the Penal Code.

153 Art. 142, para. 4 of the Penal Code.

154 Art. 142, para. 3 of the Penal Code.

155 *Hrvatska: Poštar krivotvorio potpise a sebi uzimao penzije* (Postman forged signatures and took pensions to himself), Informer.ba, 02.08.2011. [Online] Available at: https://informer.ba/tekstovi/vijesti/hrvatska-postar-krivotvorio-potpise-sebi-uzimao-penzije/ (Accessed: 30 March 2022).

156 Judgement of the Municipal Criminal Court in Zagreb K-238/2017 (12.3.2020.); and uphleding judgement of the County Court in Šibenik Kž-215/2020.

In the case of *Taylor-Sabori v. the United Kingdom*,[157] the ECtHR found a violation of Art. 8 when police intercepted the applicant's pager messages, which were the basis for a conviction because of the absence of any legal regulations on such interception.

### *3.3. Unauthorized audio recording and eavesdropping*

Unauthorized Audio Recording and Eavesdropping[158] can be committed by one who audio records without authorization another person's privately uttered words or by means of special devices eavesdrops without authorization another person's privately uttered words that are not intended to be heard by him/her,[159] alternatively, whoever uses or makes available to a third party the recorded words referred to in para. 1[160] or whoever publicly reveals the eavesdropped words literally or in essential outlines.[161]

In other words, the perpetrator is the person who records non-publicly spoken words that are meant to him but not to others. Therefore, if someone records his conversation on the cell phone without knowledge and the consent of the other participant in the conversation, person who is recording is committing a criminal offence. However, when the perpetrator records a non-public statement intended for him, it will not necessarily be a criminal offense, if he/she is recording criminal offence e.g., threat. In that case it will represent the reasons for excluding unlawfulness (e.g., recording a threat).[162]

The perpetrator must be aware of the lack of consent of the person being recorded or wiretapped, as well as the fact that the spoken words are not intended for the public (and in the case of wiretapping, the words are not intended for him or her), and must act with intent regarding this element.[163]

For this criminal offence is important that the words are not meant for the public. Spoken words as *Martinović and Tripalo* state "are non-public when they are not directed or understandable to an unlimited number of persons or a wider circle of unrelated persons."[164]

In addition, the perpetrator is a person who unauthorizedly eavesdrops "privately spoken words of another that are not intended for him or her" using special devices, or disseminates recorded or heard words.

157 ECtHR case *Taylor-Sabori v. the United Kingdom, (*Appl. no. 47114/99), 22 October 2002, (Final 22.01.2003), §§17–19. [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Taylor-Sabori%20v.%20the%20United%20Kingdom%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-60696%22]} (Accessed: 15 May 2022).

158 Art. 143 of thePenal Code.

159 Art. 143, para. 1 of the Penal Code.

160 Art. 143, para. 2 of the Penal Code.

161 Art. 143, para. 2 of the Penal Code.

162 See Dragičević Prtenjača, 2014, p. 172.

163 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, pp. 169–170.

164 Martinović and Tripalo, 2017, p. 501.

Which sort of special devices can be used is not stated, but it is clear that "ordinary" eavesdropping on other people's conversations (e.g., through closed doors, in public places, etc.) is not a criminal offense. For this form of criminal offence, it is important to establish that the words of the wiretapped person are not intended for either the perpetrator or the public. The perpetrator must know that the words were unauthorizedly sound recorded. It is not necessary for the person to whom the recording was made available to be truly acquainted with its contents, but it is enough for it to be made possible.

If someone disseminates heard words, it is not necessary to literally transmit another's statement to the public. It would be sufficient that it is presented in essential outlines, i.e., the basic content. In this case, too, the perpetrator must be aware that someone else's statement was obtained through unauthorized eavesdropping.

The sentence, which can be imposed, are fine and imprisonment for a term of up to three years.[165]

*Modus operandi* constitutes four different ways: a) recording other people's spoken words that are not intended for the public; b) eavesdropping on others with special devices; c) by using the recordings thus obtained or giving them to other persons; d) public disclosure of other people's words obtained by eavesdropping.[166] For all these forms' prosecution can start only if there is a valid request.[167]

The aggravated form of this offence depends on the special characteristics of the perpetrator. Therefore, if this offence is committed by an official exercising his or her official duty, or by a public official in the exercise of public authority, then it is considered more serious and the sentence is imprisonment between six months and five years,[168] and is prosecuted on an *ex officio* basis.

The criminal offence of Unauthorized Audio Recording and Eavesdropping protects the privacy of another person. Therefore, by the decision of the Croatian Supreme Court,[169] when a person records himself, consciously or unconsciously there will be no such criminal offence.[170] In addition, it can be committed only against natural person.[171]

Recording or eavesdropping must be unauthorized. In the literature, the meaning of the term "unauthorized" is disputed, so some authors (*Pavišić, Grozdanić and Veić*) consider recording unauthorized primarily "when it is performed outside the

165 Art. 143, para. 1 of the Penal Code.
166 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 168.
167 Art. 143, para. 5 of the Penal Code.
168 Art. 143, para. 3 of the Penal Code.
169 Decision of the Supreem Court of Republic of Croatia (VSRH), no. I Kž-1092/06 "The Supreme Court of the Republic of Croatia, as a court of second instance: the protection of privacy from interference with technical devices for audio-visual recording has been established to prevent unjustified intrusion into another person's private life. Protection does not include actions taken by that person himself, knowingly or unknowingly, because such protection of privacy cannot be imagined."
170 Dragičević Prtenjača, 2014, p. 173.
171 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 168.

cases allowed by law"[172] and by some other authors (*Bačić and Pavlović*)[173] when it is recorded or eavesdropped upon without consent of the person. The author of this Chapter gives her own solution to the meaning of the "unauthorized," combining those two stand points.[174] In any case, when the recorded or eavesdropped person gives his consent for the recording or eavesdropping, there will be no violation of his privacy, so the essence of the act will not be realized.[175]

Croatian Penal Code knows the exclusion of the unlawfulness regarding this criminal offence. Therefore, there will be no criminal offense when the acts of unauthorized sound recording or wiretapping were committed in in the public interest or another interest prevailing over the interest to protect the privacy of the person being recorded or eavesdropped on.[176]

This means although someone else's privacy has been violated, there will be no criminal offence, due to the public interest or some other interest which prevails the interest of the recorded person. This is known as reason of exclusion of unlawfulness. In addition, it must be noted how there is no definition nor mutual understanding due to the notions of "the public interest or other interest." However, such decision on prevailing interests should be assessed in concerto, weighing the interests in each case.

Unlawfulness can also be ruled out based on general provisions of the Croatian Penal Code, (necessity or self-defense), but also based on other laws as well, e.g., Criminal Procedure Act (CPA), the Police Act (PA),[177] the Police Affairs and Powers Act (PAPA),[178] the Security and Intelligence System of the Republic of Croatia Act (SISA)[179] and other laws, due to the unity of the legal order.[180] Therefore, the person who conducts a special action according to Art. 332 CPA will not be committing this criminal offence.[181]

All unauthorized recordings, as well as the special devices will be confiscated due to the special provision in this Art. (para. 6) although it could also be confiscated according to Art. 79. PC (provision in general part of the Penal Code), but due to the provision of this article, special devices and recordings will be mandatorily confiscated regardless of whether there is a danger of reuse of such recordings and devices. The *ratio* of these provisions, however, is the same as the *ratio* of the Art. 79 PC—to prevent new potential breaches of privacy by continuing use of such recordings.[182]

172 Pavišić, Grozdanić and Veić, 2007, p. 369.
173 Bačić and Pavlović, 2004, p. 546.
174 Dragičević Prtenjača, 2014, pp 179–185.
175 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 169.
176 Art. 143, para. 4 of the Penal Code.
177 The Police Act, Official Gazette, 34/11, 130/12, 89/14, 151/14, 33/15, 121/16, 66/19.
178 The Police Affairs and Powers Act, Official Gazette, 76/09, 92/14, 70/19.
179 The Security and Intelligence System of the Republic of Croatia Act, Official Gazette, 79/06, 105/06.
180 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 169.
181 Ibid. p. 169.
182 Ibid. p. 170.

### *3.3.1. Case law*

#### 3.3.1.1. National case law—Constitutional court of the republic of Croatia

There was an interesting case where the Constitutional Court of the Republic of Croatia (U-III/244/1997) has quashed the Decision of the State Judicial Council and the Decision of the Sabor (Croatian Parliament), because the applicant was relieved of his duties as president and judge of the Supreme Court of the Republic of Croatia when he was caught in special evidentiary actions which were not intended to him.[183] The Constitutional Court found that the applicant's right to a fair trial[184] , the right to privacy in the form of personal, family life, dignity, honor, and reputation[185] , the right to privacy in correspondence and other forms of communication[186] and the right to privacy, security, and secrecy of personal data[187] had been violated.[188]

#### 3.3.1.2. European Court of human rights case law

The ECTHR decisions regarding this issue of unauthorized audio recording or eavesdropping, are mainly related to issues of procedural law and law guaranteed in criminal proceedings.[189] However, it is necessary to mention two key cases that have arisen before the Court; *Klass and Others v. Germany*[190] and *Malone v. the United Kingdom*,[191] in which the ECtHR ruled on the quality of the law and the compatibility of its provisions with those of the Convention.

In *Klass and Others v. Germany*, the applicants argued that laws allowing the authorities to supervise individuals without informing them constituted a violation of Art. 8. The Court found that the law governing the supervision of individuals was sufficient, defined, and precise and that the procedure governing supervision and ensuring that all supervision measures are in accordance with the law and provisions of the Convention. Therefore, it concluded how there is no violation of Art. 8 of the Convention.[192]

183 Decision of the Constitutional Court, no. U-III/244/1997., p. 3., also see Dragičević Prtenjača, 2014, p. 176.
184 Art. 29 of the Constitution.
185 Art. 35 of the Constitution.
186 Art. 36 of the Constitution
187 Art. 37 of the Constitution.
188 Dragičević Prtenjača, 2014, p. 176.
189 Dragičević Prtenjača, 2014, p. 174.
190 Judgement ECtHR *Klass and Others v. Germany* (Appl. no. 5029/71, 6 September 1978 https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22klass%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57510%22]} (Accessed: 29 March 2022).
191 Judgement ECtHR *Malone v. the United Kingdom,* (Appl. no. 8691/79), 2 August 1984; [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22malone%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57533%22]} (Accessed: 29 March 2022).
192 *Klass and Others v. Germany,* paras. 45, 46, 56.

He took a different position in *Malone v. the United Kingdom* in which he found a violation of Art. 8 because "surreptitious surveillance"[193] of applicants was carried out during the criminal investigation in the form of police interception of telephone conversations (tapping) and recording of calls (listing numbers dialed from a particular telephone).[194] The Court found that the legislation and regulation concerning police wiretapping, is not precise and specific enough to comply with Art. 8 of the Convention. Therefore, the wiretapping and recording of calls and the use of such information, without sufficient legislation governing such conduct or without the consent of the person whose calls are recorded, constitute unjustified invasion of privacy and violation of Art. 8 of the Convention.[195]

The Court found a violation of Art. 8 of the Convention in a series of cases because the laws or bylaws that regulated the problem of wiretapping did not comply with the provisions of Art. 8 §2 of the Convention, for example in *Huvig v. France*,[196] *Kruslin v. France*, [197] *Khan v. the United Kingdom*[198] (2000), etc.

In *Craxi v. Italy* (no. 2) (2003),[199] the Court found a violation of Art. 8 of the Convention even in when information was obtained in a lawful manner, concerning the reading-out in court and the disclosure in the press of transcriptions of a politician's telephone conversations, intercepted in the context of criminal proceedings for corruption. Information was released to the public but respect for the rights of the individual was not ensured because the authorities failed to prohibit journalists' access to transcripts of private telephone conversations. Therefore, the ECtHR took position that the authorities had a positive obligation to prevent the release into the public domain of the private conversations.

In the *Kruslin v. France,*[200] the court stated, *inter alia,* "recording and other forms of interception of telephone conversations (wiretapping) constitute a serious

193 *Malone v. the United Kingdom,* para. 39.

194 *Malone v. the United Kingdom,* paras. 67, 68, 87.

195 *Malone v. the United Kingdom*.

196 Judgement ECtHR *Huvig v. France* (Appl. no. 11105/84)), 24 April 1990; [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22huvig%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57627%22]} (Accessed: 28 March 2022).

197 Judgement ECtHR *Kruslin v. France* (Appl. no. 11801/85), 24 April 1990, §35, [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Kruslin%20v.%20France%22],%22itemid%22:[%22001-57626%22]} (Accessed: 28 March 2022).

198 Judgement ECtHR *Khan v. the United Kingdom* (Appl. no. 35394/97), 12 May 2000, Final (04/10/2000); [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22khan%20v%20united%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58841%22]} (Accessed: 29 March 2022).

199 Judgement ECtHR *Craxi v. Italy* (no. 2) (Appl. no. 25337/94), 17 July 2003 (final 17/10/2003, §§68–76; [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Craxi%20v.%20Italy%22],%22itemid%22:[%22001-61229%22]} (Accessed: 28 March 2022).

200 Judgement ECtHR *Kruslin v. France* (Appl. no. 11801/85), 24 April 1990, §35, [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Kruslin%20v.%20France%22],%22itemid%22:[%22001-57626%22]} (Accessed: 28 March 2022).

interference with private life and correspondence and must therefore be based on particularly precise law."[201] It is extremely important that there are clear, detailed rules on this issue, especially as available technology becomes more sophisticated,"[202] and found a violation of Art. 8 of the Convention. The Court considered how "the legislation governing wiretapping was not clear and specific enough" and it did not provide sufficient protection rights from possible abuses, i.e., the applicant did not enjoy even the minimum degree of protection to which citizens in a democratic society would be entitled.[203]

In the case of *P.G and J.H. v. the United Kingdom,*[204] the Court found a violation of Art. 8. The police kept special concealed audio recordings of persons answering police questions, and use them and the information obtained, for further analysis without informing those persons of the actions taken during that investigation process.[205]

### *3.4. Unauthorized taking of pictures*

The unauthorized taking of footage includes taking pictures[206] of another person located in a dwelling or an area especially protected from view without authorization, or uses or makes it available to a third party such a picture, thus violating the person's privacy for which a prison sentence of up to one year is prescribed,[207] and this primarily form shall be prosecuted upon request.[208] The perpetrator can be anyone taking the picture or who uses or disseminates picture obtained in this way.[209] Yet aggravated form of this offence must be committed by persons with the special characteristics e.g., "official person in exercising its official duty or by a public official in the exercise of public authority" and the perpetrator can be sentenced to imprisonment for a term of up to three years.[210]

The act of committing this offence is proscribed alternatively; so, it consists of photographing another who is in an apartment or space protected from view, or from using the recording thus obtained, or from giving the recording thus obtained to another person.

To be protected from view, it must be filmed in an apartment or other space truly protected from view—a hotel room, a fenced yard, a shower cabin, bathroom, hatchery, solarium, etc., and even an outdoor pool on private property if it is protected

201 *Kruslin v. France*, §33.
202 *Kruslin v. France,* §33.
203 *Kruslin v. France*, §§33, 36.
204 Judgement ECtHR *P.G and J.H. v. the United Kingdom* (Appl. no. 44787/98), 25 September 2001, Final (25/12/2001); [Online] Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59665%22]} (Accessed: 29 March 2022).
205 *P.G and J.H. v. the United Kingdom,* para. 63, see also: Dragičević Prtenjača, 2014, p. 175.
206 Art. 144 of the Penal Code.
207 Art. 144, para. 1 of the Penal Code.
208 Art. 144, para. 3 of the Penal Code.
209 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 172.
210 Art. 144, para. 2 of the Penal Code.

from view.[211] *Munivrana Vajda* believes that only filming that violates the right to privacy—primarily the right to privacy and family life[212]—or only cases of violation of the most intimate sphere, should constitute a criminal offense,[213] and may be punishable. Therefore, by such interpretation, taking pictures of someone doing usual actions, e.g., cleaning or vacuuming in her/his home, would not constitute a criminal offense. The author disagrees with this view.

The crime must be committed with intent, and *Munivrana Vajda* believes that unauthorized does not refer to the will or knowledge of the person being filmed, but to "protection from view," i.e., the space that is protected from view.[214] The method of recording is not relevant—it is only important that it is a visual recording.

The manner and content of the consent, but also the content of the recording, are of great importance not only for the existence of criminal offenses of unauthorized recording, but also for the issue of liability for damage under civil law regulations.

The Media Act (MA) prescribes the publisher's liability for damages. The release of the publisher from liability for damage is regulated in Art. 21, para. 4

> if the information with which the damage was done is a photograph of the injured party taken in a public place or a photograph of the injured party taken with his knowledge and consent for publication, and the injured party did not prohibit publication, i.e., limited the right of the author of the photograph to exploit the work.[215]

It is evident from the cited provision that one of the exculpatory reasons is the fact that the photograph was taken in a public place. Any recording in a public place cannot be this offence.[216] There is a fiction that refers to it being shown in public, so it is considered that whoever is in a public place agrees to be filmed. This fiction is disputable, but that is current situation in Croatia, which is codified in the Unauthorized Taking of Pictures.[217] The MA wants to make a clear distinction between photographs taken in public places from photographs taken in non-public places or private photographs, the publication of which requires the prior consent and approval of the persons photographed.[218]

What is considered a public place is a critical issue. In Croatia, there is no unique solution, nor is this issue regulated in any of the above-mentioned laws. In *Jelušić's* opinion, a public place should be where anyone who wants to can access it freely, voluntarily, freely, and subject to certain conditions—for example, streets, squares,

211 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 172.
212 Ibid. p. 173.
213 Ibid. p. 173.
214 Ibid. p. 174.
215 Art. 21, para. 4, al. 4 of MA.
216 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 172.
217 For more see Dragičević Prtenjača, 2014, pp 164–199.
218 Dragičević Prtenjača, 2014, p. 182.

parks, public beaches, stadiums, cinemas, restaurants, etc.[219] Hence, *argumetnum a contrario,* non-public places should be all places of access that require prior approval or consent: home, private beaches, offices, etc.[220] It is also possible that part of a building is public and part a non-public place, such as banks.[221]

The assumption is that everyone who finds himself or herself in public places (public beach, stadium, theatre, park) loses the right to a part of his privacy. The reasoning for such comprehension is how there is a very high probability that person who is outside can be photographed due to the advance and available technology (cell phones etc.). This is however disputable. Also, in connection to the aforementioned standpoint there is another one regarding publishing the photographs taken in public place in the media without person's explicit consent. This reasoning is for reconsideration, but similar position was taken by the Constitutional Court in one of its decisions[222] expressing the legal view that photographs taken in public places may be freely published.[223]

It is proscribed that all pictures and special devices used for committing the criminal offence shall be seized.[224]

Sentence is lenient than for criminal offence of Unauthorized Audio Recording and Eavesdropping. *Munivrana Vajda* considers how the development of technology of video recording has become widespread phenomenon and, in many cases, an accepted phenomenon.[225]

### *3.4.1. Case law*

#### 3.4.1.1. National case law

In Croatian case law, a husband took photographs of his ex-wife while she was taking a shower with his cell phone, and then he threatened to send it to all her family, He said they will come to kill her because they are Muslims.[226] The case was rejected because the injured party withdrew her request.

In another case, a telecommunications technician was provide service to a famous person in Croatia, according to the work order that stated the celebrity's name and address. When the technician arrived, he photographed the person on the couch and posted these pictures on Facebook together with the work order containing his

219 Jelušić, 2008, p. 79.
220 Jelušić, 2008, p. 79.
221 Dragičević Prtenjača, 2014, p. 183.
222 US RH, U-III / 4365/2005.
223 See Decision of the Croatian Constitutional Court no. US RH U-III/4365/2005.
224 Art. 144, para. 4 of the Penal Code.
225 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 171.
226 Judgment of the Croatian Municipal Criminal Court in Zagreb, no. Kzd-121/2020; wife has given up further prosecution and the court brought a formal decision refusing prosecution, which was upheld by the County Court of Zagreb (no. Kžzd-199/2020).

personal data.[227] He was found guilty for the Art. 144 PC (Unauthorized Taking of Pictures) and Art. 146 PC (Unlawful Use of Personal Data).

#### 3.4.1.2. European Court of Human Rights case law

As stated above, the European Court of Human Rights has taken the standpoint in case *Niemietz v. Germany*[228] that privacy has a broad meaning and encompasses various aspects of an individual's life. The right to physical and mental integrity, sexual life, gender and sexual orientation, personal data, reputation, name, photographs, and therefore any and even visual footage that includes neutral actions (cooking, reading, etc.) could be understood as a violation of the right to privacy, and can constitute a criminal offence.

Hence, its case law regarding issue of privacy in public places differs—especially when it is a private person in a public place. In some situations, the Court considers that person can have the right to protection of privacy.

In the above-mentioned case *Peck v. the United Kingdom* (in Section 2.2, Regional Instruments),[229] the Court held there is a violation of Art. 8. The private person was recorded while attempting to commit suicide in a public place, and the Court considered since the footage is clearly focused on and related to one individual only,[230] the CCTV operator who had alerted the police and observed their intervention could have made enquiries with the police to establish the identity of the applicant and thereby request his consent to disclosure.[231]

In the case *Von Hannover v. Germany* (no. 2) (2012), the Court stated how even some public person recorded in a public place can have the right to protection of privacy and a recording may violate Art. 8 of the Convention if it was not recorded in the general/public interest, but only to entertain the reader: the reader's interest in being entertained generally carried less weight than that of protecting privacy, in which case the reader's interest did not merit protection.[232]

But in the end, the Court concluded there was not a violation of Art. 8 of the Convention,[233] as national courts had carefully weighed in the balance the publishing

227 Judgment of the Croatian Municipal Criminal Court in Zagreb, no. K-36/2019 (3.6.2020.), which become final.

228 *Niemietz v. Germany*, para. 29.

229 *Peck v. the United Kingdom,* para. 87.

230 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 53, paras. 133, 137, 234.

231 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 53, para. 234.

232 See ECtHR Judgement *Von Hannover v. Germany* (no. 2) (2012.), (Appl. nos. 40660/08 and 60641/08), 7 February 2012; paras. 31, 32 [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20VON%20HANNOVER%20v.%20GERMANY\%22%22],%22itemid%22:[%22001-109029%22]} (Accessed: 29 March 2022).

233 *Von Hannover v. Germany* (no. 2), paras. 118, 125, 126. It considered that the Federal Court of Justice upheld the applicants' request to ban the publication of two photographs that it considered not to

company's right to freedom of expression on the one hand, and the applicants' right to respect for their private life on the other there is no violation of Art. 8.[234]

In one other more recent case of *Gaughran v. the United Kingdom*,[235] in which the authorities had decided on the indefinite retention of the photograph of an individual convicted of driving with excess alcohol, in addition to his DNA profile and fingerprints,[236] the Court found a violation of Art. 8.

The Court concluded that in deciding on that retention of personal data, without reference to the seriousness of the offence and in the absence of any real possibility of review, the authorities had failed to strike a fair balance between the competing public and private interests.[237]

### *3.5. Abuse of sexually explicit footage*

Abuse of Sexually Explicit Footage[238] is a new criminal offence introduced into the Croatian Penal Code with amendments in 2021. It was introduced because there were some cases, which were very serious but could not be qualified as any criminal offence. After the termination of the relationship, one ex-partner shared intimate photos or videos of the other ex-partner on the Internet, without the partner's consent and knowledge. They can then use the intimate footage to blackmail, belittle, or retaliate after the breakup, and can result in controlling and manipulation of the recorded person with the goal of embarrassing and humiliating the victim. This can be done in an existing relationship as well, with the goal not to determine the relationship or to manipulate with the person to do what another partner wants. In addition, many people publish such films on social networks, most often videos of ex-partners set up out of revenge. In the public, this criminal offence is known as "revenge porn."[239]

---

contribute to matters of general interest. However, he rejected the applicants' request to ban the publication of a third photo showing the application walking during a skiing holiday in St. Moritz and which was accompanied by an article on, among other things, the deteriorating health of Prince Rainer—Von Hannover v. Germany (no. 2), para. 117.

234 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 20, para. 67.

235 See ECtHR Judgement *Gaughran v. the United Kingdom* (Appl. no o. 45245/15), 13 February 2020, Final (13/06/2020) [Online] Available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Gaughran%20v.%20the%20United%20Kingdom%22],%22itemid%22:[%22001-200817%22]} (Accessed: 29 March 2022).

236 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), p. 19, para. 63.

237 Guide to the Case Law of the of the European Court of Human Rights—Data protection (last updated on 31 December 2021), pp. 19–20, para. 63.

238 Art. 144a of the Penal Code.

239 M.V., Osvetnička pornografija postaje kazneno djelo: Bivšim partnerima od života su napravili pakao, sada im prijeti višegodišnji zatvor, Dnevnik.hr; od dana 22. prosinca 2022.; dostupno na. [Online] Available at: https://dnevnik.hr/vijesti/hrvatska/osvetnicka-pornografija-novo-kaznenodjelo---688113.html (Accessed: 15 March 2022).

Considering that, in July 2021, the Abuse of Sexually Explicit Footage was stipulated as criminal offence. The perpetrator can be anyone who abuses the relationship of trust and without the consent of the filmed person makes available to a third party a recording of sexually explicit content recorded with the consent of that person for personal use and thus violates that person's privacy.[240]

The proscribed sentence is imprisonment for up to one year. The same punishment is stipulated for other *modus operandi* when someone creates new (fake) footage or alters an existing recording of sexually explicit content and uses that recording as real, thereby violating the privacy of the person on that recording via computer system.[241] The aggravated form of the offence is when both offences (in paras. 1 and 2) are committed via a computer system or network or in any other way due to which the recording became available to a larger number of persons, and the perpetrator can be punished by imprisonment for up to three years.[242]

The criminal offence is committed when the consequence occur which consists of a violation of privacy. If there are no such consequences, and the perpetrator acts with intent which must include the fact of abuse of trust and consent of the person being filmed, it would be an attempt that is not punishable given the prescribed penalty.[243] This incrimination refers also to the betrayal of trust, and confidence which must exist at the time when a picture was taken or a recording was made.

All forms of the offence are to be prosecuted upon request,[244] and all recordings and special devices with which the criminal offense was committed shall be seized.[245]

There where such cases before the amendments in 2021, and it tried to be incriminated and prosecuted under the Art. 144 PC (Unauthorized Taking of Pictures). There were problems in the prosecution, and usually it did not end well for the victim because the victim her-/himself) agreed to the (video) recording or taking pictures, so charges for this incrimination were in the most cases rejected. If Art. 144 PC is to be applied, the consent of the victim must not exist.

There was one case where victim was unconsciousness and while she was unconsciousness, her ex-partner raped her with a vibrator and took pictures of the act, after which he sent it to all their friends via WhatsApp. Among other charges, he was charged for Unauthorized Taking of Pictures[246], and the Municipal Criminal Court in Zagreb ruled against that charge, and the perpetrator of that act was found not guilty, but the appeals court in Dubrovnik upheld the verdict.[247] This was the case where

240 Art. 144a, para. 1 of the Penal Code.
241 Art. 144a, para. 2 of the Penal Code.
242 Art. 144a, para. 3 of the Penal Code.
243 Vlada Republihe Hrvatske, Prijedlog Zakona o izmjenama i dopunama Kaznenog zakona, s konačnim prijedlogom zakona, Zagreb, lipanj 2021, (Government of the Republic of Croatia, Final Draft of the Law on Amendments to the Criminal Code, Zagreb, June, 2021.) p. 18.
244 Art. 144a, para. 4 of the Penal Code.
245 Art. 144a, para. 5 of the Penal Code.
246 Art. 144 of the Penal Code.
247 Verdict of the Municipal Court in Zagreb, no. K-1156/2018 which was upheld by the County Court in Dubrovnik no. 75/2021.

there was no consent; it was done in the privacy of the ex-partner's apartment, in the bedroom, so from this fact, such a court ruling is very interesting, even then when at the time there was no special offence of the Abuse of Sexually Explicit Footage[248].

It must be added that in 2004, the "Severina" case attracted a great deal of publicity because her intimate video recording had been made available to the public.[249] She never got to criminal court, but today, the release of that intimate video would constitute a criminal offence: Abuse of Sexually Explicit Footage.

### *3.6. Unauthorized disclosure of a professional secret*

The essence of this criminal offence is unauthorized disclosure of a professional secret[250] by some persons of special profession. Therefore, certain persons to whom information on the personal or family life of another person has been entrusted in the performance of their profession can only commit it as an attorney-at-law, notary public, health worker, psychologist, employee of a welfare institution, religious confessor, or another person who discloses without authorization a piece of information about the personal or family life confided to him/her in the performance of his/her occupation,[251] and the perpetrator can be sentenced to imprisonment for a term of up to one year.[252]

The general clause regarding perpetrators of this offence ("another person" to whom secret information has been entrusted in connection with her profession will also be liable for this offense) has been retained,[253] because it is impossible to predict all the professions in the future that may exist with this obligation.

Every behavior of the person by whom a secret is transmitted, expressed, or made available to another, breaking professional secrecy, constitutes this offence. Professional secrecy can be revealed not only by verbal testimony, but as *Munivrana Vajda* notes also by (intentionally) "leaving an unprotected secret document in a place where it is available to unauthorized third parties, publishing information in professional or scientific work and in other ways."[254]

Every piece of information on personal or family life entrusted to the perpetrator of this offence in the performance of his profession is considered a professional secret.[255]

248 Art. 144a of the Penal Code.

249 Fotografije gole Severine preplavile su Internet, a seksi kadrovi mnoge su podsjetili na skandal iz 2004. godine kada je u javnost procurila snimka seksa pjevačice i njezinog tadašnjeg partnera, 21.08.2018, Net.hr [Online] Available at: https://net.hr/hot/zvijezde/severina-opet-na-udaru-nakon-objave-pornica-bila-je-u-depresiji-sada-joj-je-ponovno-zadan-udarac-2a26e85a-b1c3-11eb-94cc-0242ac14001e (Accessed: 21 March 2022). Severina is famous Croatian singer.

250 Art. 145 of the Penal Code.

251 Art. 145, para. 1 of the Penal Code.

252 Art. 145, para. 1 of the Penal Code.

253 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, pp 175–176.

254 Ibid. p. 175.

255 Ibid. p. 175.

Data comprehend any written, photographed, drawn, recorded document by any means or unwritten communication by any other means or record of data, or spoken word.[256]

By this incrimination, as well as other incriminations in this chapter the right to privacy is protected, specifically the right of citizens to the secrecy of data on personal and family life. It must be also noted how this incrimination indirectly protects the proper functioning of certain services and activities based on a relationship of trust.[257] Therefore, the duty to keep confidential information is prescribed by other laws and regulations governing the performance of these activities. Therefore, according to Art. 13 of the Advocacy Act (AA),[258] a lawyer is obliged, in accordance with the law, to keep secret everything that the party has entrusted to him or that he has learned in another way in representing the party,[259] and other persons who work or have worked in a law office are also obliged to keep attorney–client confidentiality.[260]

Similarly, in Medical Act stipulates the obligation of a doctor to keep everything he learns about a patient who seeks medical help in connection with his health condition must be kept as a medical secret and may be disclosed.[261]

This criminal offence is committed when the disclosure of secrets is unauthorized, and primarily indicates the lack of consent of the person to whose personal and family life the information provided relates.[262] Also, other persons may be authorized to give consent for their disclosure, e.g., a doctor may disclose a medical secret unless otherwise provided by a special law, only with the approval of the patient, parent, or guardian of minors, and in the event of mental incapacity or death, with the approval of the patient's immediate family, guardian, or legal representative.[263]

The perpetrator must act with intent and must be aware of the confidential nature of the information as well as the possibility of his behavior revealing that information to another person, and he must at least agree to it. Indirect intent is not enough, and a person who reveals a secret by accident or negligence does not commit a criminal offense under this article.[264]

The PC stipulates a special reason for excluding unlawfulness. VAs it does in the criminal offense of Unauthorized Audio Recording and Eavesdropping[265], it states that there shall be no criminal offence referred to in paragraph 1 of this article if the secret was disclosed in the public interest or the interest of a third party, which prevails over the interest of keeping the secret.[266]

256 Ibid. p. 175.
257 Ibid. p. 176.
258 The Advocacy Act (AA), Official Gazette, 09/94, 117/08, 50/09, 75/09, 18/11, 126/21.
259 Art. 13, para. 1 of AA.
260 Art. 13, para. 2 of AA.
261 Art. 21 of MA.
262 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 176.
263 Art. 21 of MA.
264 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 177.
265 Art. 143, para. 4 of the Penal Code.
266 Art. 145, para. 2 of the Penal Code.

However, unlike Art. 143, para. 4 PC, which deals with the general interest, Art. 145, para. 2. PC speaks about the interest of another person, which is more important than the interest of secrecy or protection of privacy. *Munivrana Vajda* states how "an example of the public interest is the interest in detecting a criminal offense, while the interest of another person is, for example, its protection from a dangerous contagious or sexually transmitted disease."[267] Therefore, the conflicting interest of the public or another person on the one hand and the secrecy on the other should be considered in each case *in concerto* depending on the circumstances of the individual case.

Giving the fact that unlawfulness can be excluded if there is a consent of the person whose data are in question as well as if there is a consent of another person who is authorized to give the consent in the name of that person, unlawfulness can also be excluded when other laws prescribe such possibility.[268] This necessarily stems from the unity of the legal order.[269] This criminal offence as many other for this chapter is to be prosecuted upon request.[270]

In another case, an attorney gave a client's letter to the prosecution (state attorney's office) in which the client threatened to kill another attorney representing him in come civil law cases. His attorney represented him in a civil law case as well. Both the municipal and the county court in Varaždin decided there was not breach of law and the criminal offence under Art. 145. Unauthorized Disclosure of a Professional Secret was not committed. Reasoning was that his lawyer was only for civil law cases, and the sever threat is one of the reasons from Art. 145. para. 2 PC.[271]

### *3.7. Unlawful use of personal data*

Unlawful Use of Personal Data[272] criminalizes the actions anyone who "in contravention of the conditions set out in the Act, collects, processes, or uses personal data of physical persons," and the stipulated sentence for this basic form of the offence is fine or imprisonment for a term of up to one year. [273] This is the most frequent offence in our case law[274].

The object of protection is personal data, i.e., the inviolability of personal data, which may not be used outside the purpose established by law without the authorization of that

267 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 177.

268 E.g., "A doctor is obliged to report to the police or the state attorney's office when, during the performance of medical activity, he suspects that a person has died or was injured by force. The doctor is also obliged to submit the report referred to in para. 1 of this article when he suspects that the health or condition of a minor or infirm person is seriously endangered by neglect or abuse."—Art. 22, paras. 1–2 of MA.

269 Munivrana Vajda, 2018, cited in Cvitanović et al., 2018, p. 177.

270 Art. 145, para. 3 of the Penal Code.

271 Decision of the Municipal Court in Varaždin, Kž-48/18-4 (30.1.2018.).

272 Art. 146 of the Penal Code.

273 Art. 146, para. 1 of the Penal Code.

274 See chapter 4. Statistical Analyses.

person.[275] Personal data is any information relating to an identified natural person or the natural person who can be identified. Personal data is defined in the GDPR, and concerns any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[276]

By *Pavišić and Grozdanić* a person can be identified if his identity can be established directly or indirectly based on one or more characteristics specific to his physical, psychological, mental, economic, cultural, or social identity.[277] The protection is for personal data of any natural person, regardless of the fact whose citizen it is.[278]

The ECJ in *Nowak*[279] concluded that personal data consist of the answers of the candidate at a professional examination, and comments of the examiner's regarding those answers.[280]

In *Buivids*[281] the ECJ stated that the recorded images of police officers in a police station constitute personal data; therefore, it concluded that it is possible to see and hear the police officers in the video in question, so those recorded images of persons constitute personal data within the meaning of Art. 2(a) of Directive 95/46.[282]

The processing of data comprehends different actions. The GDPR defines it as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, regarded as alignment or combination, restriction, erasure, or destruction.[283]

ECJ case law in *Buivids*[284] "processing of personal data," is defined in Art. 2(b) of Directive 95/46 as "any operation or set of operations which is performed upon personal data…such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or

275 Pavišić, Grozdanić, and Veić, 2007, p. 371.
276 Art. 4(1) of the GDPR.
277 Pavišić, Grozdanić and Veić, 2007, p. 371.
278 Konačan prijedlog Kaznenog zakona s obrazloženjem, Vlada Republike Hrvatske, Zagreb, [Final proposal of the Criminal Code with explanation, Government of the Republic of Croatia] p. 189. [Online] Availbale at: https://sabor.hr/sites/default/files/uploads/sabor/2019-01-18/080229/PZE_866.pdf (Accessed: 25 March 2022).
279 C-434/16, EU:C:2017:994.
280 Judgment of December 20, 2017, Nowak (C-434/16, EU:C:2017:994), para. 62; See also paras. 27–62.
281 C-345/17, EU:C:2019:122. Judgment of February 14, 2019, Buivids (C-345/17, EU:C:2019:122) [Online] Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=210766&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=52616 (Accessed: 15 May 2022).
282 Judgment of 14 February 2019, Buivids (C-345/17, EU:C:2019:122), para. 32.
283 Art. 4(2) of the GDPR.
284 C-345/17, EU:C:2019:122.

destruction." In the context of a video surveillance system, the Court has held that a video recording of persons which is stored on a continuous recording device—the hard disk drive of that system—constitutes, pursuant to Art. 2(b) and Art. 3(1) of Directive 95/46, the automatic processing of personal data[285].

Therefore, the ECJ concluded that the video recording which was stored in the "memory of the camera used by the applicant constitutes a processing of personal data and the act of publishing a video recording, which contains personal data, on a video website on which users can watch and share videos, constitutes processing of those data wholly or partly by automatic means."[286]

The aggravated form of the offence is when personal data are transferred outside of the Republic of Croatia for further processing, or are made public or in some other way available to a third party, or if it is acquired significant pecuniary gain for himself/herself or another, or causes considerable damage,[287] or if it is committed against a child or on whoever, in contravention of the conditions set out in the act, collects, processes, or uses personal data of physical persons on the racial or ethnic origin, political views, religious or other beliefs, trade union membership, health, or sex life or the personal data of physical persons on criminal or misdemeanor proceedings.[288]

The perpetrator can be sentenced to fine or to imprisonment for a term of up to three years.[289]

It is considered as a special aggravated offence when all the mentioned forms are committed by an official person in exercising its official duty or by a public official in the exercise of public authority.[290] Stipulated punishment is more severe than for other forms, so the perpetrator can be sentenced to imprisonment for a term of between six months and five years.

This criminal offense is very closely connected to the previous Personal Data Protection Act and today's GDPR because it depends on its provisions, but also on provisions of other acts, e.g., the Media Act, Electronic Media Act, Consumer Protection Act, Electronic Communications Act, etc., which very often indicate the application of GDPR.

By its nature, this offence is a so-called *blanket criminal offence*, because its essence cannot be known unless other laws or regulation are consulted. If there were some special reasons in the GDPR (or other laws) that allow the collecting of data in some special cases to which this incrimination refers, that would constitute the reason for excluding the unlawfulness.

Unlike most other offenses in this chapter, criminal proceedings for this offense are initiated *ex officio*.

285 See to that effect, judgment of December 11, 2014, *Ryneš*, C-212/13, EU:C:2014:2428, paras. 23, 25. Judgment of 14 February 2019, Buivids (C-345/17, EU:C:2019:122), paras. 33 and 34.

286 Court of Justice of the European Union, Fact sheet — Protection of Personal Data, pp. 16–17.

287 Art. 146, para. 2 of the Penal Code.

288 Art. 146, para. 3 of the Penal Code.

289 By Art. 40 of the Penal Code. When a prison sentence up to three years is prescribed, then a provision should be read that a fine or sentence of three months to three years can be imposed.

290 Art. 146, para. 4 of the Penal Code.

### *3.7.1. Case law — National courts*

According to conducted research at the Zagreb Municipal Criminal Court, the author found there are many these criminal offences that were in concurrence of the offence[291] with others; e.g., fraud[292] or some offences of forgery (e.g., Forging of Documents Art. 278. PC or Forging Official or Business Documents Art. 279 PC, etc.). From conducted research at Zagreb Municipal Court as well as from data of the Croatian Bureau of Statistics (CBS; see Chapter 4), it is obvious that this crime is very common in practice.

In one case, a person was stopped by the police for drunk driving[293] and presented a false personal data identity card—that of his brother (and the brother did not give permission for usage). After that, he signed the arrest report and the notice of the misdemeanor with his brother's name. He was accused and convicted for Concurrently Adjudicated Criminal Offences (Concurrence of Offences) of Unlawful Use of Personal Data[294] and forging documents[295]. He was sentenced to unique sentence of 10 months' imprisonment; he was given a suspended sentence with two years' probation time.[296] Therefore, instead of only committing the misdemeanor, by giving the false personal data he committed not one, but two criminal offences. Also, it must be noted, in the author's opinion, there has been a wrong qualification of the offense. Therefore, instead of the Art. 146. it should be qualified as another criminal offense Misuse of identity document Art. 280.

In another case, someone committed the Continuing Criminal Offence of Unlawful Use of Personal Data[297,298] and Fraud[299].[300] A perpetrator got personal data

291 Art. 51 of the Penal Code. Concurrently Adjudicated Criminal Offences (Art. 51 of the Penal Code). "(1) If the perpetrator commits by one act or more acts several criminal offences for which he/she is tried concurrently, the court shall first fix the sentence for each criminal offence and then, based on its assessment of the perpetrator's personality and the committed criminal offences in their totality, impose upon him/her an aggregate sentence.
(2) The aggregate sentence shall be set by increasing the highest individual sentence incurred. It must, however, be less than the sum of individual sentences and must not exceed the maximum limit for long-term imprisonment or a fine.
(3) Where individual sentences of long-term imprisonment the sum of which exceeds fifty years have been imposed for two or more criminal offences, the court may pronounce an aggregate sentence of long-term imprisonment for a term of fifty- years.
(4) Where sentences of imprisonment and fines have been imposed as individual sentences, the court shall pronounce an aggregate sentence of imprisonment and an aggregate fine.
(5) Where paragraphs 2 and 4 of this Art. are being applied, the sentence of juvenile imprisonment shall be equated with the sentence of imprisonment."

292 Art. 236 of the Penal Code.

293 Judgement of the Municipal Criminal Court in Zagreb, K-1496/2020, 20. 08. 2020, p. 1.

294 Art. 146, para. 1. of the Penal Code.

295 Art. 278, para. 1, 3. of the Penal Code.

296 Judgement of the Municipal Criminal Court in Zagreb, K-1496/2020, 20. 08. 2020, p. 2.

297 Art. 146, para. 1. of the Penal Code.

298 There was seven such offences which were decided to be prosecuted as one continuing criminal offence.

299 Art. 236 of the Penal Code.

300 There were five offences of fraud which was decided to be prosecuted as one continuing criminal offence.

from the vehicle sales contract between his father and another person. He ordered several smartphones in the name of the third person, with 24-month contracts, pocketing 47 thousand KN (approx. 6 thousand euros or USD $6,500). He was sentenced to one-year imprisonment with Community Service[301].[302]

One case with the similar *modus operandi* was in K-2045/18 where the perpetrator was as an employee of a telephone company in Croatia, and used the same approach to order several cell phones.[303] He was accused and convicted for the concurrence of the continuing offence of the Unlawful Use of Personal Data[304], continuing offence of the Abuse of Position and Authority[305] and continuing offence of the Forging Official or Business Documents[306]. He got 11 months of imprisonment modified into the Community Service.[307]

The most interesting case was the one with more than 20 criminal offences, which were qualified as the offence of the continuing Unlawful Use of Personal Data[308], continuing offence of the Abuse of Position and Authority[309] and continuing offence of the Forging Official or Business Documents[310].[311] There were three perpetrators acting in organization of these offences but not always together. Usually there were two of them. One of them was the employee of one Telecommunication Company, which procured the data of the subscribers, and then transferred that data to the other person, which called the telecommunication company and made subscription contracts to the names of the others. All perpetrators got suspended sentence or Partial suspended sentence.[312]

301 Art. 55 of the Penal Code.
302 Judgement of the Municipal Criminal Court in Zagreb, K-729/17, 2.11.2017.; The Judgement was final on December 20th, 2017.
303 Judgement of the Municipal Criminal Court in Zagreb, K-2045/18, 28.2.2020.
304 Art. 146, para. 1 of the Penal Code.
305 Art. 291, para. 1 of the Penal Code.
306 Art. 279, para. 1 of the Penal Code.
307 Judgement of the Municipal Criminal Court in Zagreb, K-2045/18, 28.2.2020, p. 2.
308 Art. 146, para. 1 of the Penal Code.
309 Art. 291, para. 1 of the Penal Code.
310 Art. 279, para. 1 of the Penal Code.
311 Judgement of the Municipal Criminal Court in Zagreb, K-1522/16, 27.02.2018. which was upheld by County Court in Split Kž-363/2018.
312 Partial suspended sentence is when perpetrator must serve one time of the custodial sentence in prison, and other part of the sentenced is like plain, regular suspended sentence (Art. 57 of the Penal Code). Partial Conditional Sentence:
"(1) The court may impose upon a perpetrator sentenced to a fine or a term of imprisonment of a minimum of one year and a maximum of three years a conditional sentence for only a part of the sentence if it deems that there is a high degree of probability that even if the entire sentence is not executed, the perpetrator will commit no further criminal offences.
(2) The unconditional part of a prison sentence shall not be less than six months nor more than one half of the pronounced sentence term.
(3) The unconditional part of a fine shall not be less than one fifth nor more than one half of the pronounced sentence.
(4) The provisions on parole shall not apply to the unconditional part of the prison sentence.
(5) The provisions of Articles 56, 58, 62, 63 and 64 of this Act shall apply accordingly to the conditional part of the sentence.."

In accordance with the above, we can indeed ask ourselves what is the purpose of punishment in the mentioned cases and whether it is achieved.

### *3.8. Other criminal offences regarding violation of the right to privacy in other chapters of the Croatian Penal Code*

In Croatian criminal law and the Penal Code, there are some other criminal offences which directly or indirectly protect the right to privacy and can be found in other chapters of the PC then the chapter "Criminal Offences against Privacy." One of these offences is Violation of the Privacy of the Child[313] which is in the chapter "Criminal Offences against Marriage, Family, and Children"; and other is Disclosing the Identity of a Person at Risk or Protected Witness[314], which is in the chapter "Criminal Offences against the Judiciary".

#### *3.8.1. Violation of the privacy of the child*

Child privacy is under special protection by the Convention on the Rights of the Child[315] and other international and regional documents which guarantee privacy rights of all people. Croatian Penal Code also protects the privacy of the child as a special criminal offence by its Art. 178.

This criminal offence of violation of the child's privacy may commit anyone (even parents) if they disclose or transmit something from the child's personal or family life, publish a child's photograph or reveal the child's identity contrary to regulations, which caused the child anxiety, ridicule of peers or other persons or otherwise endangered the child's welfare.[316]

The perpetrator can be punished (for this basic form) by imprisonment for a term not exceeding one year.[317]

If it is done in public or in such manner that privacy of the child becomes available to a larger number of people, it constitutes the aggravated form of the offence and a stipulated sentence is imprisonment for up to two years.[318] Another aggravated form which is even more serious is if it is done by an official person or in the performance

313 Art. 178 of the Penal Code.

314 Art. 308 of the Penal Code.

315 Art. 16: 1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation.
2. The child has the right to the protection of the law against such interference or attacks.—Art. 16 of Convention on the Rights of the Child (1989) [Online] Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (Accessed: 5 May 2022).

316 Art. 178, para. 1 of the Penal Code.

317 Art. 178, para. 1 of the Penal Code.

318 "Whoever commits the act referred to in para. 1 of this Art. through the press, radio, television, computer system or network, at a public gathering or in any other way due to which it has become accessible to a larger number of persons, shall be punished by imprisonment for up to two years." — Art. 178, para. 2 of the Penal Code.

of a professional activity, and stipulated sentence is imprisonment for a term not exceeding three years.[319]

It must be noted how many parents are not thinking about what can happened when they are putting pictures of their children without their "consent"[320] on Facebook, Instagram, or other platforms. By such doing, they can violate the right of the privacy of their children. Of course, not every violation of the child's privacy is automatically criminal offences, but in some cases, it can constitute one. Some actions if it leads to the child anxiety, ridicule of peers or other persons or otherwise endangered the child's welfare can have constituted this criminal offence (Violation of the Privacy of the Child).

In Croatian case law by data of the Croatian Bureau of Statistics (CBS) in period 2016–2020 there has been only nine convictions.[321]

There was an interesting case in the ECtHR case law regarding the privacy rights of the child who was a victim of the criminal offence. The ECtHR case *Kurier Zeitungsverlag und Druckerei GmbH v. Austria*, 2012[322] protected the right to privacy and personal data of victims private and family life. In this case prevailed the protection of private life guaranteed in Art. 8 (right to respect for private and family life) over Art. 10 (freedom of expression). The applicant in the present case published two articles in its newspaper with a lot's of personal data about the case[323] and minor victim who has been sexually abused by her father and her stepmother who were convicted of aggravated sexual abuse of minors, deliberate aggravated bodily harm and ill-treatment of minors and sentenced them to fifteen years' imprisonment. Therefore, the minor victim filed a claim for compensation on the ground that the articles by the applicant company had revealed her identity as the victim of a crime. The national Austrian courts ruled in her favor, so the ECtHR has found no violation of Art. 10.

319 "Whoever commits the act referred to in paragraphs 1 and 2 of this Art. as an official person or in the performance of a professional activity, shall be punished by imprisonment for a term not exceeding three years." — Art. 178, para. 3 of the Penal Code.

320 It is for a debate can the children give consent, and from which age. In Croatian criminal law when children are the victims, the person is considered to be a child by the age of the 18.—Art. 113, para. 2 of The Juvenile Courts Act, Official Gazette, 84/11, 143/12, 148/13, 56/15, 126/19.

321 Database 2016–2020, Information [Online] Available at: https://dzs.gov.hr/ (Accessed: 5 April 2022). Remark: there has been an enormous change regarding this site, and the interface of the Croatian Bureau of Statistics, and for a great deal of time there was a different link, and data were available in different forms and reports than today.

322 *Kurier Zeitungsverlag und Druckerei GmbH v. Austria*, (Appl. no. 3401/07), 17 January 2012 (Final 17/04/2012), paras. 13–21. and 47–56. [Online] Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-108689%22]} (Accessed: 15 May 2022).

323 Kurier gave detailed descriptions of the circumstances of the case and revealed victims identity by mentioning her first name, the full names of her father and stepmother, their family relation and publishing photographs of them.

*3.8.2. Disclosing the identity of a person at risk or protected witness*

This criminal offence is primarily regulated for the protection of the efficiency of the criminal proceedings ("*Criminal Offences against the Judiciary*"), and secondary because of the violation of the privacy of the person. Yet it remains the fact that private data and personal life must be protected. A perpetrator of this offence is

- whoever imparts or hands over to another or publishes without authorization information on the identity of a person at risk, or
- a person who has been or will be questioned as a protected witness, or
- with respect to whom the procedure for inclusion in the witness protection program pursuant to a special act has been instituted, or
- who has been included in the witness protection program, or
- whoever takes any other action with the aim of disclosing information on the identity of this person or with the aim of tracking down this person.[324]

Therefore, the modality of the offence is the publication or dissemination of personal information regarding the identity of the person at risk or protected witness with the goal to find that person or reveal data which could lead to revealing her/his identity. That could be any sort of action with any means, to reveal the identity of the person, and to make a disturbance in the criminal proceedings and the evidentiary process, and in the ends in trial and has an effect on the verdict and judgement. Sentence is imprisonment for a term of between six months and five years.[325]

By the data of the Croatian Bureau of Statistics, there has not been any convictions for this criminal offence in the observed period (2016–2020).

## 4. Statistical analysis

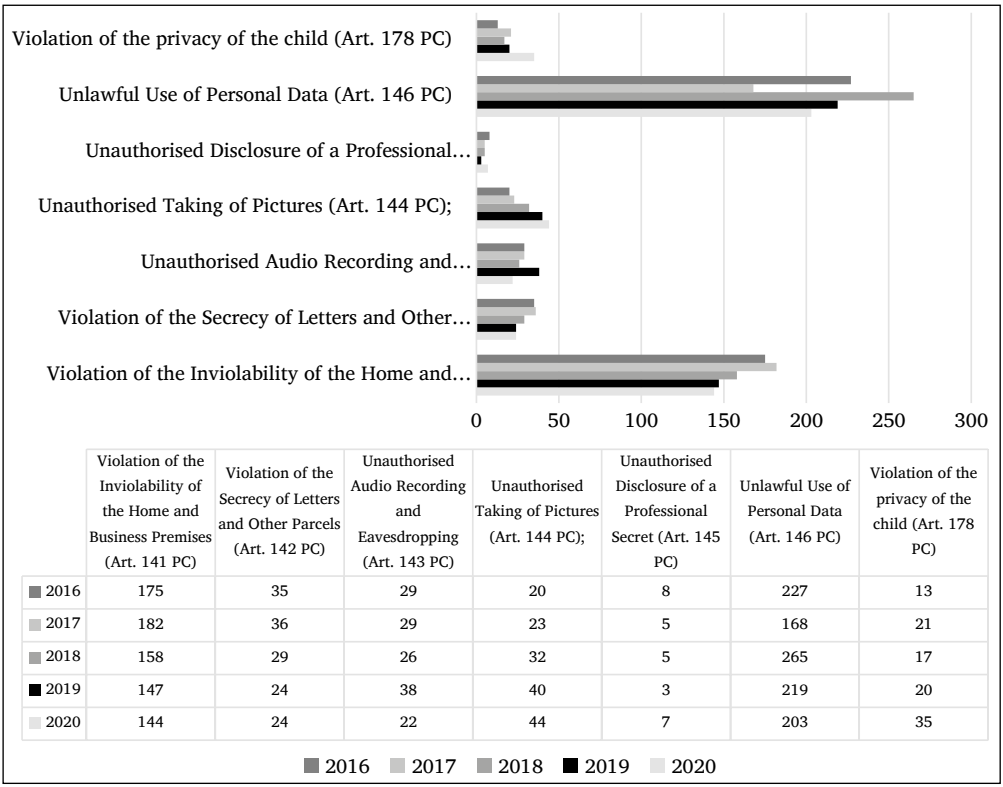
Some statistical data needs to be presented and analyzed. The Croatian Bureau of Statistics were consulted for 2016–2020, regarding criminal offences against privacy and violation of the privacy of a child[326] to observe the situation at national level. In parallel, the author conducted the research at the Zagreb Municipal Court regarding criminal offences in the chapter "Criminal Offences against Privacy" in the same period (2016–2020) to see and compare figure trends at both the local and national level.

324 Art. 308 of the Penal Code.
325 Art. 308 of the Penal Code.
326 Art. 178 of the Penal Code.

### *4.1. Data of the Croatian Bureau of Statistics*

Data from the Croatian Bureau of Statistics (CBS) in (2016–2020) will be observed in relation to criminal offences against privacy[327] and Violation of the Privacy of the Child[328] and the imposed sentences. Abuse of Sexually Explicit Footage[329] has been a criminal offence since July 2021; as of this writing, there has not yet been any case law.

According to the analyzed data. the most frequently reported crime in the observed period is Unlawful Use of Personal Data[330], followed by Violation of the Inviolability of the Home and Business Premises[331], and almost the same pattern can be seen for accused persons[332], and convicted persons[333].



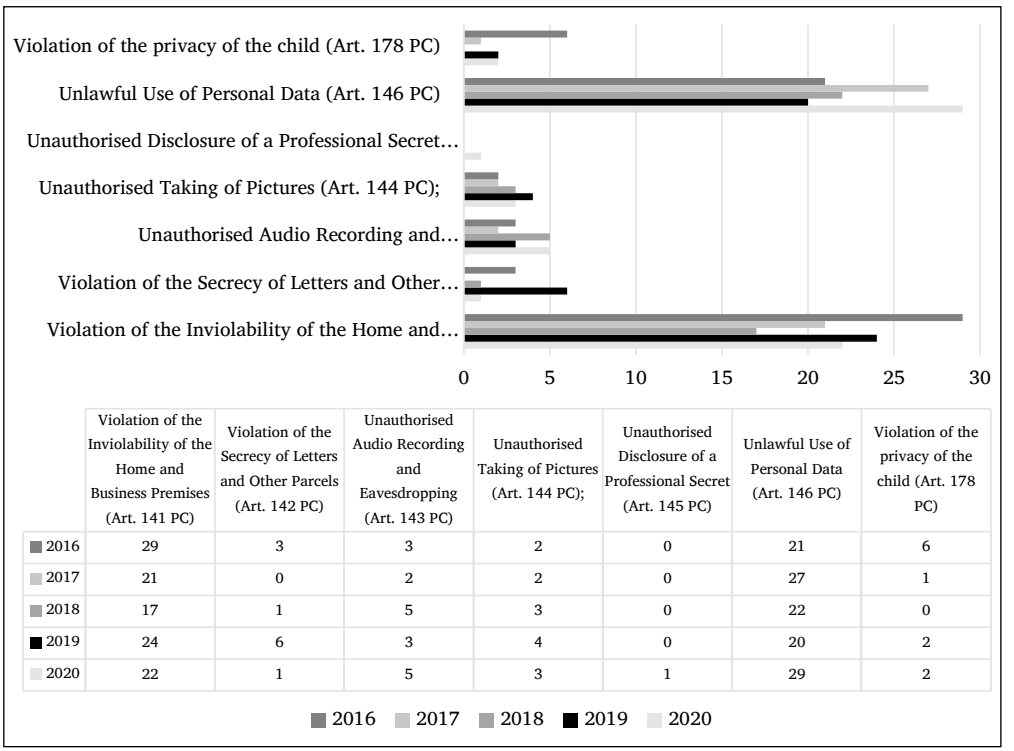

| | Violation of the Inviolability of the Home and Business Premises (Art. 141 PC) | Violation of the Secrecy of Letters and Other Parcels (Art. 142 PC) | Unauthorised Audio Recording and Eavesdropping (Art. 143 PC) | Unauthorised Taking of Pictures (Art. 144 PC); | Unauthorised Disclosure of a Professional Secret (Art. 145 PC) | Unlawful Use of Personal Data (Art. 146 PC) | Violation of the privacy of the child (Art. 178 PC) |
|---|---|---|---|---|---|---|---|
| 2016 | 175 | 35 | 29 | 20 | 8 | 227 | 13 |
| 2017 | 182 | 36 | 29 | 23 | 5 | 168 | 21 |
| 2018 | 158 | 29 | 26 | 32 | 5 | 265 | 17 |
| 2019 | 147 | 24 | 38 | 40 | 3 | 219 | 20 |
| 2020 | 144 | 24 | 22 | 44 | 7 | 203 | 35 |

2016 2017 2018 2019 2020

*Figure 1: Reported adult persons by criminal offences (Arts. 141–146 PC and Art. 178 PC) for 2016–2020*

327 Arts. 141–146 of the Penal Code.
328 Art. 178 of the Penal Code.
329 Art. 144a of the Penal Code.
330 Art. 146 of the Penal Code.
331 Art. 141 of the Penal Code; See Figure 1.
332 See Figure 2.
333 See Figure 3 and Table 1.

Figure 1 shows that there is no clear trend line among all criminal offences. However, criminal offences that are decreasing are Violation of the Secrecy of Letters and other parcels[334], Unauthorized Audio Recording and Eavesdropping[335] with the exception of 2019, while Unauthorized Taking of Pictures[336] and Violation of the Privacy of the Child[337] increased from 2016 until 2020. The least represented criminal offence is Unauthorized Disclosure of a Professional Secret[338].




| | Violation of the Inviolability of the Home and Business Premises (Art. 141 PC) | Violation of the Secrecy of Letters and Other Parcels (Art. 142 PC) | Unauthorised Audio Recording and Eavesdropping (Art. 143 PC) | Unauthorised Taking of Pictures (Art. 144 PC); | Unauthorised Disclosure of a Professional Secret (Art. 145 PC) | Unlawful Use of Personal Data (Art. 146 PC) | Violation of the privacy of the child (Art. 178 PC) |
|---|---|---|---|---|---|---|---|
| 2016 | 29 | 3 | 3 | 2 | 0 | 21 | 6 |
| 2017 | 21 | 0 | 2 | 2 | 0 | 27 | 1 |
| 2018 | 17 | 1 | 5 | 3 | 0 | 22 | 0 |
| 2019 | 24 | 6 | 3 | 4 | 0 | 20 | 2 |
| 2020 | 22 | 1 | 5 | 3 | 1 | 29 | 2 |

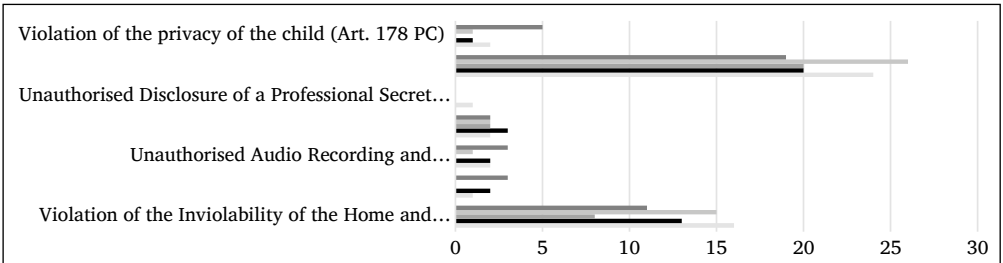
2016 2017 2018 2019 2020

*Figure 2: Accused adult persons by criminal offences (Art.141–146 PC and Art. 178 PC) for 2016–2020*

The same distribution can be seen among reported and accused person for selected criminal offences. Most frequent criminal offences are Unlawful Use of Personal Data[339] and Violation of the Inviolability of the Home and Business Premises[340]. All other criminal offences are represented in a very small share if any, as in the case

334 Art. 142 of the Penal Code.
335 Art. 143 of the Penal Code.
336 Art. 144 of the Penal Code.
337 Art. 178 of the Penal Code.
338 Art. 145 of the Penal Code.
339 Art. 146 of the Penal Code.
340 Art. 141 of the Penal Code.

of Unauthorized Disclosure of a Professional Secret (Art. 145 PC, only one accused in 2020). There is high difference in absolute numbers between reported and accused person for the represented criminal offences[341].




| | Violation of the Inviolability of the Home and Business Premises (Art. 141 PC) | Violation of the Secrecy of Letters and Other Parcels (Art. 142 PC) | Unauthorised Audio Recording and Eavesdropping (Art. 143 PC) | Unauthorised Taking of Pictures (Art. 144 PC); | Unauthorised Disclosure of a Professional Secret (Art. 145 PC) | Unlawful Use of Personal Data (Art. 146 PC) | Violation of the privacy of the child (Art. 178 PC) |
|---|---|---|---|---|---|---|---|
| 2016 | 11 | 3 | 3 | 2 | 0 | 19 | 5 |
| 2017 | 15 | 0 | 1 | 2 | 0 | 26 | 1 |
| 2018 | 8 | 0 | 0 | 2 | 0 | 20 | 0 |
| 2019 | 13 | 2 | 2 | 3 | 0 | 20 | 1 |
| 2020 | 16 | 1 | 2 | 2 | 1 | 24 | 2 |

2016 2017 2018 2019 2020

*Figure 3: Adult persons convicted of criminal offences (Arts. 141–146 PC and Art. 178 PC) for 2016–2020*

Figure 3 presents the number of convicted adults for selected criminal offences for 2016–2020. The trend is almost the same as for the reported and accused persons. The most frequent offence is Unlawful Use of Personal Data[342], followed by Violation of the Inviolability of the Home and Business Premises[343]. Other criminal offences are represented with very small shares. Only for Unauthorized Taking of Pictures[344] is there at least one convicted person in each year. In total, there have been 198 convicted persons for criminal offenses against privacy[345] plus nine (9) for Violation of the Privacy of the Child[346] in 2016–2020 in Croatia. Altogether there have been 207 convicted persons.

In 2020 there is at least one person convicted for all observed criminal offences. There is a significant representation of criminal offence of Unlawful Use of Personal

341 See Figure 1 and 2.
342 Art. 146 of the Penal Code.
343 Art. 141 of the Penal Code.
344 Art. 144 of the Penal Code.
345 Arts. 141–146 of the Penal Code.
346 Art. 178 of the Penal Code.

Data[347]. It makes more than 50% of the convictions for privacy criminal offences. Violation of the Inviolability of the Home and Business Premises[348] makes up more than 30% of the convictions for those criminal offences, and only those two criminal offences make more than 80% of all convictions for privacy criminal offences. The privacy criminal offences account for less than 0.4% (46 in total) of all convictions of adult perpetrators in 2020 (in total 11,634).

*Table 1: Convicted persons for criminal offences against privacy (Art. 141–146. PC and Art. 178 PC) in 2016–2020 in Croatia*

| Criminal offence / Year | 2016 | 2017 | 2018 | 2019 | 2020 | In total |
|---|---|---|---|---|---|---|
| **Violation of the Inviolability of the Home and Business Premises (Art. 141 PC)** | 11 | 15 | 8 | 13 | 16 | **63** |
| **Violation of the Secrecy of Letters and Other Parcels (Art. 142 PC)** | 3 | 0 | 0 | 2 | 1 | **6** |
| **Unauthorized Audio Recording and Eavesdropping (Art. 143 PC)** | 3 | 1 | 0 | 2 | 2 | **8** |
| **Unauthorized Taking of Pictures (Art. 144 PC);** | 2 | 2 | 2 | 3 | 2 | **11** |
| **Unauthorized Disclosure of a Professional Secret (Art. 145 PC)** | 0 | 0 | 0 | 0 | 1 | **1** |
| **Unlawful Use of Personal Data (Art. 146 PC)** | 19 | 26 | 20 | 20 | 24 | **109** |
| **Violation of the Privacy of the Child (Art. 178 PC)** | 5 | 1 | 0 | 1 | 2 | **9** |

It is obvious from the presented data in Figure 4, how there has been the most suspended sentences for the Unlawful Use of Personal Data[349] in total 96 suspended sentences which is in line with the general data of the CBS on convictions. It is followed by suspended (imprisonment) sentences for Violation of the Inviolability of the Home and Business Premises[350] with 55 in total. There were fewer than ten imprisonment sentences for other criminal offences against privacy.

347 Art. 146 of the Penal Code.
348 Art. 141 of the Penal Code.
349 Art. 146 of the Penal Code.
350 Art. 141 of the Penal Code.

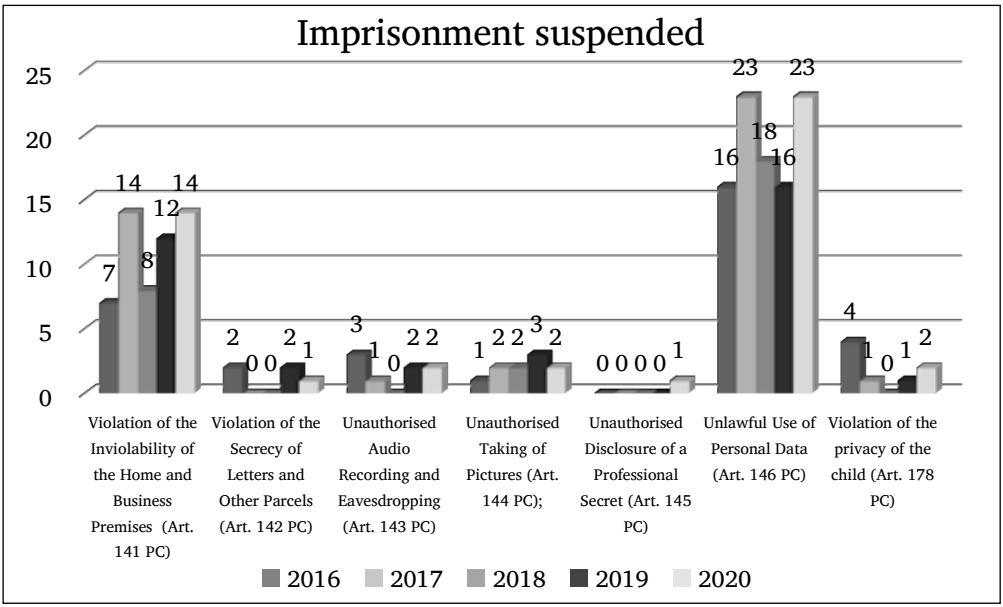



*Figure 4: Convicted adult persons by pronounced imprisonment suspended (suspended imprisonment sentence) for criminal offences (Arts. 141–146 PC and Art. 178 PC) for 2016–2020*

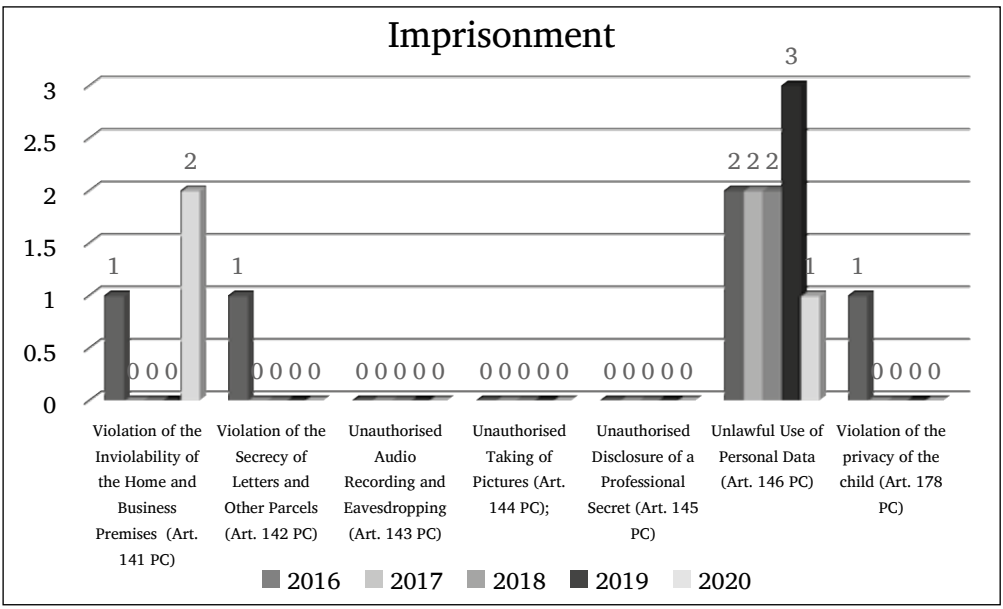



*Figure 5: Convicted adult persons by pronounced imprisonment for criminal offences (Art. 141–146 PC and Art. 178 PC) for 2016–2020*

Figure 5 presents pronounced imprisonments for selected criminal offences from 2016 until 2020. Convicted adult persons were sentenced to imprisonment only for Violation of the Inviolability of the Home and Business Premises[351] and Unlawful Use of Personal Fata[352], with exception in 2016 in which one person was sentenced to imprisonment for Violation of the secrecy of letters and other parcels[353]. Therefore, for selected criminal offences the most frequent penalty is suspended imprisonment in all five years.

### *4.2. Research — Zagreb Municipal Criminal Court*

The author of the report conducted the research at Zagreb Municipal Criminal Court for criminal offences against privacy[354] for 2016–2020. There have been 16 cases of offences against privacy.

*Table 2: Cases of criminal offences against privacy (Art. 141–146 PC) in 2016–2020—Zagreb Municipal Criminal Court[355]*

| Criminal offence / Year | 2016 | 2017 | 2018 | 2019 | 2020 | In total |
|---|---|---|---|---|---|---|
| **Violation of the Inviolability of the Home and Business Premises (Art.141)** | 1 | 0 | 0 | 0 | 1 | **2** |
| **Violation of the Secrecy of Letters and Other Parcels (Art.142)** | 0 | 1 | 0 | 0 | 0 | **1** |
| **Unauthorized Audio Recording and Eavesdropping (Art.143)** | 0 | 0 | 0 | 0 | 0 | **0** |
| **Unauthorized Taking of Pictures (Art.144)** | 1[356] | 1 | 0 | 0 | 1[357] | **3** |
| **Unauthorized Disclosure of a Professional Secret (Art.145)** | 0 | 0 | 0 | 0 | 0 | **0** |
| **Unlawful Use of Personal Data Art.146** | 0 | 1 | 3 | 0 | 6 | 10 |

351 Art. 141 of the Penal Code.
352 Art. 146 of the Penal Code.
353 Art. 142 of the Penal Code.
354 Arts. 141–146 of the Penal Code.
355 Art. 144a of the Penal Code is criminal offence since June 2021, therefor there is no decisions of the courts yet.
356 Kzd-121/2020.
357 In case K-36/19 one perpetrator is convicted for concurrence of the offence of the Arts. 144 and 146 of the Penal Code; therefore there is one judgment for two criminal offences.

Hence, there have been 12 convictions, but 11 persons were convicted. The reason lies in fact that one person was convicted in one judgement for concurrence of the two offences against privacy[358].[359] There have also been two acquittals at Zagreb Municipal Criminal Court, for Art. 144 PC in the case K-1156/2018 and for Art. 142 in the case K-238/2017. Two formal decisions (Verdict Dismissing the Charges)[360] were made in case Kzd-121/2020 for Art. 144 PC and in case KMp-105/2016 for Art. 141 PC.

The most common criminal offense at Zagreb Municipal Criminal Court is Unlawful Use of Personal Data (Art.146) which constitutes 83% of all convictions for criminal offenses against privacy.

*Table 3: Convicted persons for criminal offences against privacy (Arts. 141–146 PC) for 2016–2020 in the Zagreb Municipal Criminal Court[361]*

| Criminal Offence / Year | 2016 | 2017 | 2018 | 2019 | 2020 | In total |
|---|---|---|---|---|---|---|
| **Violation of the Inviolability of the Home and Business Premises (Art. 141)** | 0 | 0 | 0 | 0 | 1 | **1** |
| **Violation of the Secrecy of Letters and Other Parcels (Art. 142)** | 0 | 0 | 0 | 0 | 0 | **0** |
| **Unauthorized Audio Recording and Eavesdropping (Art. 143)** | 0 | 0 | 0 | 0 | 0 | **0** |
| **Unauthorized Taking of Pictures (Art. 144)** | 0 | 0 | 0 | 0 | 1[362] | **1** |
| **Unauthorized Disclosure of a Professional Secret (Art. 145)** | 0 | 0 | 0 | 0 | 0 | **0** |
| **Unlawful Use of Personal Data Art. 146** | 0 | 1 | 3 | 0 | 6 | **10** |

358 Art. 144 and Art. 146 of the Penal Code.
359 In case K-36/19.
360 Similars are Dismissing Judgement and Judgement Refusing a Charge.
361 Art. 144a of the Penal Code is criminal offence since June 2021, therefore there is no convictions of the courts yet.
362 In this case one perpetrator is convicted for concurrence of the offence of the Arts. 144 and 146 of the Penal Code (K-36/19).

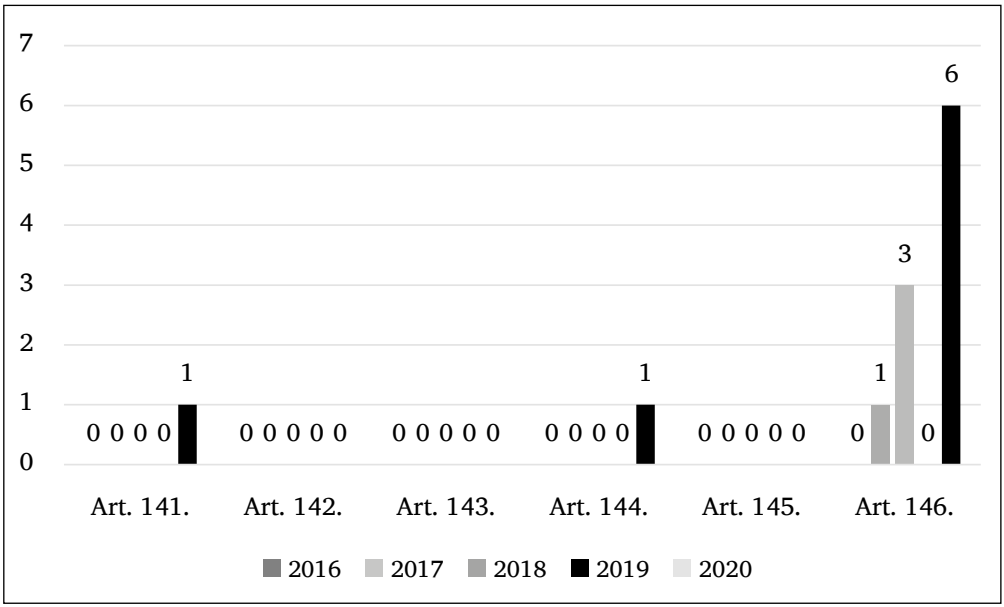



*Figure 6: Convicted persons for criminal offences against privacy (Arts. 141–146. PC) for 2016–2021 at the Zagreb Municipal Criminal Court*

Some of the offences against privacy in the research were in concurrence of the offences with some other offences e.g., Fraud[363] and Forging Documents[364] or Forging Official or Business Documents[365]. Only in one case, at the Zagreb Municipal Criminal Court, there has been the concurrence of the two criminal offences against privacy[366].[367] Distribution of data show the similar pattern as on the national level. The most frequent criminal offence is Unlawful Use of Personal Data[368] which is followed with Violation of the Inviolability of the Home and Business Premises[369] and Unauthorized Taking of Pictures[370].

363 Art. 236 of the Penal Code.
364 Art. 278 of the Penal Code.
365 Art. 279 of the Penal Code.
366 Art. 144, 146 of the Penal Code.
367 As it was mentioned in case K-36/19.
368 Art. 146 of the Penal Code.
369 Art. 141 of the Penal Code.
370 Art. 144 of the Penal Code.

## 5. Final remarks

Collecting on other people's data, without their knowledge is actually spying. This is the right word to use for describing what is happening. Many people do not think about these aspects—maybe they do not want that, maybe they are not aware of the danger that is present in every day visit to Internet or by doing some legal actions (e.g., conclusion of the contract when they are providing their personal data). Maybe they do not want to think about it. But want it or not, the danger is present, and we are leaving our (personal) data signature about are habits, wishes, interests in everyday life to all sorts of persons (physical or legal) and entities. Banks are collecting our data, as are news portals, websites, journals, almost everybody. All use that information for different purposes, unilaterally deciding to store, sort, and even "sell it to the highest bidder."

The people, the law, the regulators have recognized this (collecting personal data of another which is in the essence of the privacy), as a problem. They are trying, if not to prevent it, then at least regulate it, as better as it is possible. It is done in different areas e.g., civil law but also criminal law as well. The GDPR is trying to regulate issue of the collection of our personal data, but many of us willingly give or share our personal data on various platforms. Its general goal is to protect the personal data of natural persons, to provide citizens with control over their personal data and to create a high and uniform level of data protection.[371]

Croatia deals with this issue of protection of the right to privacy and established a special agency (the Croatian Personal Data Protection Agency) for monitoring the application of the GDPR. The criminal law comes at the end as *ultima ratio*, when adequate protection was not accomplished in other legal branches and by other laws. Therefore, criminal offences exist. In Croatian criminal law, one chapter contains most of the privacy criminal offences. In that regard author wanted to see how many such criminal offences were committed in the period 2016–2020. By data collected both by the Croatian Bureau of Statistics and by research conducted at the Zagreb Municipal Criminal Court, the most frequent criminal offence is Unlawful Use of a Personal Data[372] which is represented in more than 50% of the convictions for criminal offences against privacy (by CBS data) and 83% by research at the Zagreb Municipal Criminal Court. It is followed by Violation of the Inviolability of the Home and Business Premises[373], around 30% by CBS data, but not so much according to our research at the Zagreb Municipal Court (only 0.8%). In the CBS data the convictions of Unauthorized Taking of Pictures[374] constitute around 5% of the convictions. Interestingly, there are no data in the observation period for Disclosing the Identity

371 Information [Online] Available at: https://azop.hr/osnovne-informacije-za-organizacije/ (Accessed: 25 April 2022).
372 Art. 146 of the Penal Code.
373 Art. 141 of the Penal Code.
374 Art. 144 of the Penal Code.

of a Person at Risk or Protected Witness[375]. Abuse of Sexually Explicit Footage[376], also known as "revenge porn," is still a "young" criminal offence (since July 2021), so it is understandable that there is no data for convictions for that criminal offence.

In the end despite the commendable effort of the different regulators, documents, and even legislation the great responsibility is on us. We must be careful in leaving our personal trace in everyday life, especially on Internet, because we can become victims of criminal offences and perpetrators.

375 Art. 308 of the Penal Code.
376 Art. 144a of the Penal Code.

# Bibliography


ARCHARD, D. (2006) 'The Value of Privacy', in CLAES, E., DUFF, A., GUTWIRTH, S. (eds.) *Privacy and the Criminal Law*. 1st edn. Antwerpen: Intersentia, pp. 13–31.

BAČIĆ, F., PAVLOVIĆ, Š. (2004) *Komentar kaznenog zakona*. Zagreb: Organizator.

BOBAN, M. (2012) 'Pravo na privatnost i prao na pristup informacijama u suvremenom informacijskom društvu'*, Zbornik radova Pravnog fakulteta u Splitu*, 49(3), pp. 575–598.

BOJANIĆ, I., CVITANOVIĆ, L., DERENČINOVIĆ, D., GROZDANIĆ, V., KURTOIVĆ, A., NOVOSELEC, P., TURKOVIĆ, K. (2011) *Posebni dio kaznenog prava* [Special part of the Criminal Law]. Zagreb: Pravni fakultet Sveučilišta u Zagrebu.

DRAGIČEVIĆ, P. M. (2014) 'Kaznena djela neovlaštenog zvučnog snimanja i prisluškivanja te neovlaštenog slikovnog snimanja s osvrtom na praksu Europskog suda za ljudska prava i elaboracijom pojmova privatnosti i neovlaštenosti', *Godišnjak Akademije pravnih znanosti Hrvatske* [Croatian Academy of Legal Sciences Yearbook]*,* 5(1), pp. 164–199.

GLANCY, D. J. (1979) 'The Invention of the Right to Privacy', *Arizona Law Review,* 21(1), pp. 1–39.

HARRIS, D. J., O'BOYLE, M., WARBRIC, C. (eds.) (2009) *The Law of the European Convention on Human Rights*. 2nd edn. Oxford: Oxford University Press.

JELUŠIĆ, D. (2008) 'Odgovornost nakladnika medija za objavu fotografija snimljenih na javnim mjestima', *Pravo i porezi*, 2008/12, pp. 77–82.

KOKOLAKIS, S. (2017) 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon'*, Computers & Security,* 64(1), pp. 122–134 [Online]. Available at: https://doi.org/10.1016/j.cose.2015.07.002 (Accessed: 11 October 2022).

MARALYAN, A. (2012) *Comparative Analysis of the Protection of Private Life of Public Officials and Public Figures Guaranteed by the Constitution of the United States and European Convention for the Protection of Human Rights and Fundamental Freedoms*. Medford: Tufts University Fletcher School of Law and Diplomacy.

MARMOR, A. (2015) 'What Is the Right to Privacy?', *Philosophy & Public Affairs,* 43(1), pp. 3–26 [Online]. Available at: https://doi.org/10.1111/papa.12040 (Accessed: 11 October 2022).

MARTINOVIĆ, I., TRIPALO, D. (2017) 'Zvučno I slikovno snimanje u kaznenom materijalnom i procesnom pravu–- teorijski i praktični izazovi novih tehnologija i zakonskih rješenja', *Hrvatski ljetopis za kaznene znanosti i praksu* [Croatian Annual of Criminal Sciences and Practice], 24(2), pp. 499–523.

PAVIŠIĆ, B., GROZDANIĆ, V., VEIĆ, P. (eds.) (2007) *Komentar Kaznenog zakona*. 3rd edn. Zagreb: Narodne novine.

VAJDA, M.M. (2018) 'Kaznena djela protiv privatnosti [Criminal offences against privacy]' in CVITANOVIĆ, L., DERENČINOVIĆ, D., TURKOVIĆ, K., VAJDA, M.M., DRAGIČEVIĆ PRTENJAČA, M., MARŠAVELSKI, M., ROKSANDIĆ VIDLIČKA, S. (eds.) *Kazneno pravo – posebni dio* [Criminal Law – Special Part]. 1st edn. Zagreb: Pravni fakultet Sveučilišta u Zagrebu, pp. 391–404.

WARREN, S.D., BRANDEIS, L.D. (1890) 'The Right to Privacy', *Harvard Law Review*, 4(5), pp. 193–220 [Online]. Available at: https://doi.org/10.2307/1321160 (Accessed: 11 October 2022).

Chapter V

# The Right to Privacy in the Digital Age from the Viewpoint of the Slovak Legal Order

Katarína Šmigová

## 1. Introduction

Privacy *per se*, according to the Oxford Dictionary, is generally understood as a state in which one is not observed or disturbed by other people; even more, it is considered to be the state of being free from public attention.[1] Keeping in mind the digital aspects of today society, it is challenging that the definition has not been changed yet, especially in relation to the observance part or to the public attention part since it is greatly present in the current discussion about protection of the right to privacy. It is one of the defining elements of today's world. In our information society, one's personal data is its integral part. There is information all around us—not only about the world but about ourselves as well. And if it is in an electronic form that is preferred today, it can be spread worldwide quicker than ever before.

It has been a part of the human rights law ever since human rights are afforded to individuals regardless of his or her approval; their guarantee depends only on the fact of a dignity of a human being, and the foundation of freedom, justice, and peace.[2] Such an understanding of the whole area of human rights protection

1 *Oxford Dictionary.* https://languages.oup.com/google-dictionary-en/.

2 See Preamble of the Universal Declaration of Human Rights, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948).

Katarína Šmigová (2023) The Right to Privacy in the Digital Age from the Viewpoint of the Slovak Legal Order. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 165–197. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_5

includes the concept of those rights being inviolable and irrevocable (no one can be deprived of these rights), inalienable (they cannot be transferred to another), imprescriptible (and therefore their duration is indefinite), and indefeasible (they exist independently of the will of the legislature who can recognize them but cannot cancel them).[3]

Despite different sources' claim of origin,[4] human rights are not only ethical or moral principles since their recognition and effective protection are one of the principles of democracy and the rule of law.[5] It is important to remember this understanding while analyzing the way most people enter the digital world, since they usually just tick to agree with terms and conditions.[6] Although they have the right to self-determination,[7] especially today, the digital world has created a virtual reality that is not only preferred in some cases but also automatically entered into without checking to see how one's information will be used. Right of an individual to informational self-determination is a right closely related to the right to privacy. It has been deeply examined in relation with the GDPR, which requires data processing in good faith and transparency only for specified, explicit, and legitimate purposes and only for the necessary time.[8] These are rules that are to be respected from companies processing personal data; however, in case an individual ticks automatically his or her consent without reading terms and conditions, it is difficult to require the real goal of the regulation under all circumstances.[9]

Although there is no particular case law of the supreme courts of the Slovak Republic in relation to the informed consent, relevant international or supranational legal acts might be helpful.[10]

3 See Art. 12 of the Constitution of the Slovak Republic, Act no. 460/1992 Coll.

4 Vršanský and Valuch, 2016, p. 200.

5 See Preamble of the European Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe Treaty Series 005, Council of Europe, 1950.

6 See Sandle, 2020. https://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127.

7 Right to self-determination in the context of this chapter is not considered to be a right to self-determination according to Art. 1 of the International Covenant on Civil or Political Rights or Art. 1 of the International Covenant on Economic, Social and Cultural Rights, but right of an individual to informational self-determination.

8 For more detailed information see the Regulation itself: *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

9 GDPR is not the first set of legal norms that aim at protection of data processing, see e.g., The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

10 Keeping in mind that the informed consent has been analyzed mostly in relation to the medical care, the GDPR application in relation to a valid consent to process personal data has been chosen since it has been elaborated more in relation to the digital world, it is so also in the academic sphere. See e.g., https://dl.acm.org/doi/pdf/10.1145/3319535.3354212.

Consent that is required today to gain access to most social media might be considered in opposition to truly valid consent according to the GDPR.[11] Although it might be given in a good faith, there are several conditions that are to be met.[12] However, they are usually fulfilled only in a theory by checking a box to agree to terms and conditions. Individuals usually know that they must be given a free choice, i.e., they must be able to refuse or withdraw their consent without being at a disadvantage. Nevertheless, in automatic acceptance, people do not check whether the organization asking for a consent requires consent to the processing of unnecessary personal data—data that is not necessary to provide searched service. Moreover, who checks not only the identity of the organization processing data, their type, and purposes for which they are being processed—and how often those checks occur—as well as whether there is the possibility of withdrawing the given consent. The data might be used also for profiling and even more that the data might be transferred to third countries that are not within GDPR application, e.g., in case that the information concerns political opinion, religion, genetic data, data concerning health, or sex life, if these have been demonstrably disclosed by the person concerned.

If one considers adoption of the GDPR as another step of privacy protection after the well-known Google case,[13] i.e., the right to be forgotten, it might still have limits. The most important limit is the one that concerns jurisdiction. There is no doubt that state jurisdiction, which is based on the territorial nature of the state respecting the physical boundaries of the country's geography, might be considered distant from the concept of digital world, the virtual nature of which is primarily based on crossing borders; for some authors, even the issue of boundlessness is included.[14] Nevertheless, it should be pointed out that both of these concepts incorporate an aspect of control; in both cases, therefore, a state must be present in relation to its jurisdiction to create and enforce law, by judicial tools if necessary.[15]

To respect the academic goal of the present project of the Central European Academy, the present chapter is not so far reaching as to analyze and offer solutions to guarantee proper application and support of the right to privacy in the digital era. The challenges of the proper use of technological conveniences and their impact in relation to an individual and his or her right to privacy far exceed the scope of this chapter. Nevertheless, this contribution aims to analyze selected aspects of the right to privacy protection in the Slovak Republic. The overall approach is taken from the constitutional point of view, since the Constitution is the fundamental law of a state. First, the term of privacy and its content and challenges of this traditional concept in terms of the digital world is analyzed; accordingly, the text of the Constitution of the

11 See Art. 5 of the GDPR.

12 See e.g., Guidelines on Consent under Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/623051.

13 Court of Justice of the European Union (Grand Chamber), Case C-131/12, Google Spain SL v Agencia Española de Protección de Datos, 13 May 2014.

14 Barlow, 1996, https://www.eff.org/cyberspace-independence.

15 Brownlie, 2013, pp. 325 et seq.

Slovak Republic and the case law of the Constitutional Court of the Slovak Republic within the determined research area is studied. The focus is given not only on the term of privacy but also on all the issues that are covered by this term in several constitutional articles, especially the right to personal honor and reputation, name protection, protection of private and family life, protection of personal data, domestic freedom, or protection of personal communication. The question is whether this framework of the constitutional protection of the right to privacy is applicable also in the case of digital age or there is something that must be improved or changed so that the protection of this right is effective. While focusing on the Constitution, other relevant provisions of selected law are examined. The selection has been taken based on the most important challenges in relation to the right to privacy within Slovak legal order and the most important achievements; existence of relevant international case law has been another important selection factor. To mention some examples, the Slovak Civil Code providing legal tools to protect the right to privacy in case of its violation is emphasized separately. Moreover, Criminal Code, Labor Code, Act on Personal Data Protection, and Act on Electronic Communications have been taken under closer scrutiny. Since the GDPR has already been profoundly analyzed because of its specific status and purpose,[16] only some of its aspects are included into this chapter as has been done e.g., in relation to a valid consent. Finally, some groups of individuals have been selected, to name employees or children as least, since these individuals prove to be vulnerable and their status has become a challenge for proper privacy protection.

To set the hypothesis of the chapter, case law and especially legislation in the Slovak Republic is reactive in the sense that it does not actively propose new solutions to challenges of the digital world, but merely applies existing tools whenever and wherever applicable. It is not a reproof—merely reflection upon the current situation, since the technical development in relation to a digital world is so intense and rapidly changing that it has many times meant that the corresponding response of the legislature is either too slow or waiting for solutions from other sources, i.e., international or supranational inspiration. Moreover, it is difficult to react when sometimes even those whose right to privacy has been violated do not know about this violation, especially when he or she has given their consent freely to interlink or even open their privacy to the digital world.

16 To specify, the regulation is directly applicable in all the EU Member States; the aim of the present research, quite opposite, is to analyze specific features of the Slovak legal framework. It is therefore enough to point out that the regulation has been adopted to answer challenges personal data protection within the digital world. The biggest change lies in its purpose to protect the personal data of European Union citizens' and residents' data, regardless of their location and where they have their registered office or server. The concept of territoriality has thus been replaced by the concept of personality, the decisive factor is the person whose data is being processed and not the location of the data itself. However, Art. 9, para. 2 e) of this regulation is important since it indicates that the ban on processing personal data does not apply in relation to specific categories of personal data, e.g., political opinion, religion genetic data, data concerning health, sex life, if these have been demonstrably disclosed by the person concerned. For more information concerning the situation in Slovakia, see e.g., Garayová, 2020.

## 2. Term of privacy within Art. 16 of the Constitution of the Slovak Republic

Neither the right to privacy nor privacy as such is defined in the Slovak constitutional framework.[17] Nevertheless, the Constitution guarantees in its Art. 16 the right of every individual to integrity and privacy. As for limitations of this right, it may be restricted only in cases specifically provided by a law.[18] So far, it is not very much different from any other national or international legal order. Nevertheless, it is rather rare that such a provision is a part of the same article as the prohibition of torture.[19] Such a systematic classification has obviously also become a challenge in relation to the interpretation of Art. 16 of the Constitution. However, the Court has explained that the constitutional protection of the right of privacy is connected with inviolability of a person, therefore privacy is associated with body integrity and material values of private nature.[20] It is true that Art. 16 of the Convention is within articles protecting physical integrity; nevertheless, the Court shares the opinion of European Court of Human Rights emphasizing that the concept of "private life" is a broad concept encompassing, *inter alia*, aspects of an individual's physical and social identity, including the right to personal autonomy, personal development, and the establishment and development of relationships with other human beings and the outside world.[21] The protection of private life must be therefore understood in a broader sense than the protection of life from publicity: it also includes the right to establish and develop relationships with other human beings, particularly in the emotional sphere, to develop and fulfill one's own personhood.[22] Art. 8 of the Convention, like Art. 2 of the Convention, implies not only the negative obligation of the state not to interfere with privacy, but also its positive obligation to effectively ensure respect for private life, which is implemented in particular by the adoption of legislation to protect privacy. For the protection of rights to be effective in practice, there must be an effective administrative and judicial apparatus within which the individual can enforce his or her rights, particularly in cases of serious violations of physical integrity of complainants.[23]

Since there is no definition of the right to privacy in the Constitution as such, there have been several attempts to provide an understanding of this right. One of the most quoted definitions is the one of the Supreme Court of the Slovak Republic, which defined it as the right of a person to decide independently, at his or

17 See e.g., Constitutional Court, II. ÚS 424/2012 from November 6, 2014, finding, para. 33.
18 See Art. 16 of the Constitution of the Slovak Republic.
19 See Art. 16, para. 2 of the Constitution of the Slovak Republic: No one shall be subjected to torture or cruel, inhuman, or degrading treatment or punishment.
20 Constitutional Court, II. ÚS 19/97 from May 13, 1997, finding, p. 17.
21 Constitutional Court, II. ÚS 424/2012 from November 6, 2014, finding, para. 34.
22 Ibid.
23 Ibid. para. 35.

her own discretion, whether and to what extent the facts of his or her private life should be disclosed to others or made public.[24] The violation of the right to privacy within this meaning is not only the unauthorized acquisition of information and knowledge about the privacy of a person, but also the unauthorized dissemination of that information and knowledge. The consequence of an unwarranted interference with the right to privacy may be a substantial diminution of dignity or esteem in society, but this consequence is not the only legally required manifestation of the seriousness of the harm caused to the individual.[25] Consequently, procedurally speaking, the individual who has suffered harm does not have an obligation to prove that the unjustified interference has resulted in a reduction in his or her dignity in society.[26]

Originally, the right to privacy concerned exclusively natural person.[27] According to the initial interpretation of the Court, constitutional protection of privacy is associated with inviolability of a person and therefore especially its body integrity is at stake.[28] Moreover, at the beginning of its decision-making activity, the Court explicitly excluded a legal person from being a subject of privacy protection according to Art. 16 of the Constitution.[29] Nevertheless, taking into account decisions of the ECtHR,[30] the case law of the Constitutional Court has reconsidered its interpretation and included legal persons under the protection of Art. 16. Furthermore, even protection to reputation has been originally provided for only natural persons. However, the Court has reconsidered its approach in this area, and has observed that legal persons deserve not only protection under the Civil Code but also under the Constitution.[31]

Moreover, the inviolability of privacy as *lex generalis* in relation to the right to privacy has included not only rights related to physical integrity but also rights protected by other articles of the Constitution. In *Niemietz*, interpretation of private life has influenced the interpretation of the inviolability of the dwelling, which is another right protected by the Constitution, since in some contexts, work may form part of a person's life to such a degree that it becomes impossible to know in what capacity he or she is acting at a given moment of time—a private or a professional one.[32]

As it has been indicated, the inviolability of the right to privacy must be applied not only by negative obligation of a atate not to interfere directly into privacy of

24 Order of the Supreme Court of the Slovak Republic No. 3 Cdo 137/2008 from 18 February 2010, p. 9.
25 Ibid.
26 Order of the Supreme Court of the Slovak Republic No. 3 Cdo 137/2008 from 18 February 2010, p. 9.
27 Constitutional Court, I. ÚS 6/97 from 23 January 1997, decision, p. 3.
28 Compare Constitutional Court, II. ÚS 19/97 from 13 May 1997, finding, p. 17.
29 Constitutional Court, I. ÚS 6/97 from 23 January 1997, decision, p. 3.
30 E.g., ECtHR, *Niemietz v. Germany*, no. 13710/88, 16 December 1992.
31 See Constitutional Court, II. ÚS 456/2018 from 26 September 2018, decision.
32 Compare ECtHR, *Niemietz v. Germany*, no. 13710/88, 16 December 1992, para. 29.

individuals, and if so, only within limits set out by law, but also by positive duties to adopt such a legal framework that fully respects and ensures respect of human rights also within private persons relations.[33] Moreover, in case of a violation, there must be a possibility guaranteed to an individual to have his or her claim of right to privacy violation inquired.

If the text of Art. 16 of the Constitution and Art. 8 of the Convention is compared, it is surprising that the Constitution does not specify legitimate aims based on which interference into the right to privacy might be justified. Since most articles of the Constitution protecting several aspects of the right to privacy miss these legitimate aims, it is understandable that the right to privacy protected by the Constitution is being interpreted as applying conditions specified by the Convention. It is the case of not only legality, since this limitation is included into the text of Art. 16 of the Convention but lacks legitimate aims and the principle of proportionality. It means that although the Convention says nothing in most of the relevant articles protecting the right to privacy in relation to legitimate aims or proportionality, the decision-making activity of the Court strictly observes the jurisprudence of the ECtHR. The material reason is obvious since they both protect the same right. Nevertheless, there is also a formal reason: the position of the Convention in the Slovak legal order. The Convention is an international treaty on human rights and fundamental freedoms that was ratified by the Slovak Republic and promulgated in a manner laid down by law, and as such it is not only a part of the Slovak legal order but also has primacy over the law, since it provides greater scope of constitutional rights and freedoms.[34]

As mentioned earlier, the right to privacy in the constitutional framework of the Slovak Republic is included in the same article as the prohibition of torture, inhuman or degrading treatment, or punishment that has been consistently reviewed in case of personal checks, isolation, and/or monitoring while being in custody. It is rather clear that the right to privacy is violated when the right to personal freedom is violated by unlawful restriction. On the other hand, it is understandable that in case of lawful detention or deprivation of liberty, one cannot argue that one's right to privacy has been violated, since in this case, loss of privacy is an integral part of the process whose goal could not be otherwise achieved.

33 Art. 1 of the European Convention of Human Rights as interpreted in *Marcx v. Belgium*, no. 6833/74, 13 July 1979. But compare *Evans v. UK*, no. 6339/05, 10 April 2007 where the ECtHR did not consider it important to specify whether it decided the case in the context of positive or negative obligations of a State.

34 Compare Art. 154c of the Constitution of the Slovak Republic.

## 3. Other aspects of the right to privacy protected by Art. 19 of the Constitution and the Civil Code

According to Art. 19 of the Convention, everyone has the right to the preservation of human dignity, personal honor, reputation, and the protection of one's good name. Moreover, everyone has the right to protection against unauthorized collection, publication, or other misuse of personal data. Finally, everyone has the right to protection against unauthorized interference in private and family life. Again, as there is no specific condition to verify the lawfulness of an interference into these rights directly in Art. 19 of the Convention, such an interference could be realized only based on law and to the extent specified by law, to achieve legitimate aims according to the Convention and, according to the Convention, to the extent necessary in a democratic society.

The way how partly complicatedly the right to privacy is protected within constitutional framework of the Slovak Republic is best illustrated by the relationship between Art. 16 covering inviolability of a person and his/her privacy and Art. 19 covering protection of human dignity, personal honor, reputation, private and family life, and personal data. Although it has been repeatedly pointed out by the Court that the Convention does not define the term of privacy and private life, the Court has also stressed several times that human rights and freedoms guaranteed by the Convention are to be interpreted and applied in the spirit of international treaties on human rights and freedoms.[35] Therefore, according to the Court case law, protection of a private life under Art. 19, para. 2 concerns protection of intangible assets of a private nature[36] and protection of privacy under Art. 16, para. 1 concerns body integrity and material values of a private nature.[37] When interpreting these articles of the Convention, the Court has emphasized several times that it has considered the case law of the ECtHR according to which "private life is a broad term encompassing, *inter alia*, aspects of an individual's physical and social identity including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world."[38] Therefore it is a broader term than privacy protected by Art. 16 of the Constitution.

Dignity of a human being is under the Convention understood as both, a value based on natural law and a source for positively guaranteed human rights,[39] and the right of an individual to have it protected. Such a protection is guaranteed by the effective positive approach of a state in relation to creation of legal framework respecting and ensuring respect of human dignity. This legal framework includes

35 See e.g., Constitutional Court, PL. ÚS 5/93 from 18 May 1994, decision, pp. 10 et seq.
36 Constitutional Court, II. ÚS 19/97 from 13 May 1997, finding, p. 18.
37 Constitutional Court, II. ÚS 19/97 from May 13, 1997, finding, p. 17.
38 ECtHR, *Evans v. United Kingdom*, no. 6339/05, April 10, 2007, para. 71.
39 See Art. 12 para. 1, first sentence of the Constitution: People are free and equal in dignity and in rights.

not only public law, such as criminal and administrative law, but also private law, especially civil law.

As it has already been indicated, Art. 19 of the Convention protects several aspects of privacy protection. Nevertheless, as the Court has already pointed out, a distinction must be made among them since all the terms, namely human dignity, personal honor, and a good reputation, mean something else.[40] Dignity protects the very essence of individual humanity from humiliation, thus protecting humanity from being only an object of power. Reputation is the perception of a person in the community, in the society, it is a social component; on the other hand, honor is on the border between social and personal, internal concept.[41]

It must be pointed out that the current understanding of the right to privacy has been influenced by the era of non-freedom.[42] According to the Court, there was no public society and therefore no public space, protection of privacy was in fact reduced to neighborhood conflicts or commune conflicts. Such a civilistic understanding must have been changed because of necessity of individuals to "breathe freely" to develop their personality, together with understanding that there is no constitutional right to be perceived in a public space entirely the way they wish.[43] Therefore, even though protection of privacy by Civil Code is broader since it includes not only protection of honor and reputation, relevant norms of the Civil Code have to be applied and interpreted in accordance with the Constitution.[44]

To explain a specific position of the Civil Code, one must analyze hierarchy of norms in the Slovak legal order. To concretize basic protection provided by the Convention, it is the Civil Code of the Slovak Republic that forms the basis of private law protection of personality rights that are a part of right to privacy, particularly its paragraphs 11–16 that protect immaterial aspects of the right to privacy.[45] According to Art. 11 of the Civil Code, the subject of protection of human personality is, in particular, life and health, civil honor and human dignity, privacy, name, and expressions of a personal nature. Moreover, Art. 12 of the Civil Code also regulates the right to the protection of personal documents, portraits, images and video and audio recordings concerning a natural person or his or her expressions of a personal nature that might be produced or used only with the consent of this person unless produced or used for e.g., official, scientific, or artistic purposes.

The means of judicial protection of an individual's personality are, first, a negative action, i.e., a demand to a court to decide upon refrainment from unjustified interference, second, a restitution action, i.e., a demand to a court to decide upon elimination of the consequences of interference and finally, a satisfactory action, i.e.,

40 Constitutional Court, II. ÚS 191/2015 from March 26, 2015, decision, p. 26.
41 Compare Ibid.
42 Constitutional Court, II. ÚS 647/2014 from September 30, 2014, judgment, p. 32.
43 Ibid.
44 Constitutional Court, II. ÚS 152/08 from 15 December 2009, finding, para. 27.
45 Act 40/1964 Coll. Civil Code.

a demand to a court to decide upon adequate satisfaction.[46] These means of judicial protection may be applied individually or cumulatively. Their cumulative application depends on the purpose, e.g., if the unjustified interference with the personal rights persists and a right to satisfaction has arisen, a negative action with a satisfactory action may be filed.

The condition for providing personality protection is unauthorized interference with his or her personal rights that must be capable of causing harm to a person's character, but existence of harm is not a condition *sine qua non*.[47]

In the context of the protection of personality rights in the media, especially social media, there is a particular clash between two rights: freedom of expression, and protection of personality.[48] It is important to refer to the international instruments by which the Slovak Republic is bound, the interpretation of the protection of personality rights should be carried out in accordance with these treaties and the case law of their courts. Freedom of expression is one of the essential foundations of a democratic society.[49] The richest source of case law on freedom of expression is the jurisprudence of the ECtHR in Art. 10 of the Convention. At the same time, the Court considers the decisions of the ECtHR in its decision-making, and this is expressly stated in its decisions.[50] Given the importance of freedom of expression, the exceptions set out in any legal regulation must be interpreted restrictively, and the necessity of each restriction must be convincingly demonstrated.

In connection with the issue of privacy protection, the Supreme Court of the Slovak Republic stated that "a wide range of manifestations and components of a natural person's private life is also reflected in the possibility of various manifestations of privacy interventions and their consequences on protected personal rights."[51] However, in general terms, as mentioned above, most conflicts concern the conflict between right to privacy and the freedom of speech. Analysis of this conflict deserves a separate contribution to the discussion.[52] If compared, both these basic rights are in general of the same importance and weight. It is therefore not acceptable to decide normatively which one is to be given priority. Although one is preceded by the other in the text of the Constitution, it does not mean that in the Convention, the right is given priority in case of a conflict. According to the Court, such an interpretation could not be accepted since any solution to a conflict of two rights guaranteed by the Constitution depends on specific circumstances of the case.[53] It is therefore up to the

46 Števček et al., 2015, pp. 82–94.
47 Števček et al., 2015, pp. 82–94.
48 Drgonec, 2013, pp. 154 et seq.
49 ECtHR, *Handyside* v. UK, no. 5493/72, 7 December 1976, para. 49.
50 See e.g., Constitutional Court, PL. ÚS 5/93 from 18 May 1994, decision, pp. 10 et seq.
51 Decision of the Supreme Court of the Slovak Republic, no. 3 Cdo 137/2008 from February 18, 2010, p. 9.
52 Within the Central European Academy project, a separate Art. will be written upon this clash between the right to privacy and the freedom of expression.
53 Constitutional Court, III. ÚS 673/2017 from November 7, 2017, decision, para. 23.

courts, when discussing a particular dispute, to determine the need to give priority to one of the protected rights by examining the degree of importance of both in the conflict of existing constitutional values.[54] It actually means that all fundamental rights and freedoms are protected only to the extent that the exercise of one right or freedom does not unduly restrict or deny another's right or freedom.[55]

If the right to privacy is claimed to have been violated, there are several issues that courts consider, such as form and content of the speech or public interest involved in case of publicly known persons, especially politicians.[56]

The right to privacy in case of politicians is a very special case of balancing privacy and public interest. In general, more publicly known the person is, more interference into his or her privacy s/he must endure. On the other hand, one should distinguish between statements of facts and evaluative judgments. As for the former, there is no violation of the right to reputation, and for the latter, opinions must meet criteria of materiality, specificity, and proportionality.[57] Especially the issue of proportionality might be at stake since even opinions within realization of the freedom of speech might have limits although persons active in public life are expected to accept critical comments more than ordinary people. As it has already been pointed out, there are limits to the freedom of speech, in the case of public persons, e.g., in relation to attacks that are aimed to influence them in the performance of their duties and to damage public confidence in them and in the office they hold.[58] Moreover, even their personal security must be considered if freedom of speech is realized in a manner that could threaten it.[59]

One of the first issues that reflect a right to privacy of every individual is the right to a name. As for the constitutional right to a name protection under Art. 19, para. 1 of the Constitution, this is elaborated in the provisions of Art. 11 of the Civil Code. According to the Court, the cited provision includes civil honor and human dignity, in addition to the protection of his/her name and expressions of a personal nature.[60] The right to name protection under the provisions of Art. 11 of the Civil Code does not differ in principle from the constitutional right to a name protection under Art. 19, para. 1 of the Constitution. The content of the right to name protection under the provisions of Art. 11 of the Civil Code is an exclusive right of a natural person to use a name, dispose of it, and prevent anybody else from using his or her name illegally, regardless of the purpose for which it would be used. This exclusive right can also be exercised by an individual by giving consent to the use of his or her name. However, someone using the name of a natural person without express consent would thus not only violate the fundamental right of an individual according

54 Constitutional Court, III. ÚS 193/2015 from May 12, 2015, decision, p. 11.
55 Ibid.
56 See Constitutional Court, III. ÚS 385/2012 from January 21, 2014, finding, p. 18.
57 Constitutional Court, III. ÚS 193/2015 from May 12, 2015, decision, p. 9.
58 See e.g., ECtHR, *Janowski* v Poland, application no. 25716/94, January 21, 1999.
59 Compare Constitutional Court, IV. ÚS 107/2010 from October 28, 2010, decision, p. 23.
60 Constitutional Court, PL. ÚS 12/97 from October 15, 1998, finding, p. 8.

to the provisions of Art. 19, para. 1 of the Constitution, but would also act in conflict with the provisions of Art. 11 of the Civil Code.[61] A natural person cannot lose a right to his or her name, and thus the right to dispose of it, by committing an offense and being punished for the offense under the Offenses Act.[62]

Right to a name and all other parts of this aspect of the privacy protection concern not only politicians but in a digital era anybody who enters digital world, either voluntarily or not. It includes consequences of the digital world substance in its broad and quick dissemination of facts and opinions. The right to name protection might be interfered with in a very profound and sometimes even unintended way. Therefore, the protection should include various forms and ways. In relation to the right to a human dignity, honor, and reputation protection it concerns especially vulnerable groups, one of which are children.

## 4. Right to privacy in digital era and children

Children are involved within constitutional private life protection from two sides. First, sometimes as victims. Generally speaking, Slovakia is a party to all the international treaties that deal specifically with the protection of children in the online world, to name the most important one, Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography. There has been general implementation procedure has been completed and child pornography and its (also online) dissemination have been made criminal.[63] Thus the most abusive forms of violation not only of the right to private life but also to privacy (separated under the Slovak Convention) have been legally processed and covered.

There are, however, other challenges to a right of a child to privacy. Although there has been no particular case law in the Slovak Republic dealing with the violation of the right to privacy of children as such, there have already been some cases on the international level,[64] and furthermore, not only purely academic discussion about how personal data of children are shared without their consent.[65] Of course, legally speaking, parents are legally responsible for their children until they become adults themselves. However, parents sometimes provide a name and even a date of birth of their children online without considering that it remains "out there" and that it can influence the future of their children in a negative way, not even speaking about pictures that might later cause humiliation feeling if found by

61 Ibid.
62 Ibid.
63 See e.g., paras. 368, 369 of the Criminal Code.
64 See e.g., ECtHR, *Reclos and Davourlis* v. Greece, no. 1234/05, 15 January 2009.
65 See e.g., Steinberg, 2017, pp. 839–884.

schoolmates.[66] At the age of four, most children are self-aware and therefore their perception of (digital) reality should be considered as well. Not only does it help to educate children about online access and communication, but it is also in their best interest.[67] Legally speaking, one might point out that it is a right exercised under the GDPR. However, GDPR application is legally binding only for members of the European Union, and in case of worldwide accessible social media, once the information crosses the EU's borders because of an automatically checked box giving consent, personal data may go to countries where they are not considered to be personal data but information provided for while exercising freedom of (parental) speech.[68]

This area is a new challenge and still under consideration. Although within the European regional system of human rights protection there have already been some cases dealing with consent in disclosure issues, most of them concern parental consent. As has already been indicated, there have already been some cases adopted on the international level. However, in *Reklos and Davourlis*, parents who claimed violation of the right to privacy of their child by taking a picture without their consent. Nevertheless, the consent of a child is to be considered as well because they have been recognized to a right to privacy themselves not only by general international treaties on human rights, such as the Convention, but also by a *lex specialis* international treaty, Convention on the Right of a Child.[69]

When speaking about children and their right to privacy, there is surely demand for their better understanding of interweaving of the real and digital world. The violation of basic human rights is forbidden in both; nevertheless, it might have broader consequences in the digital world because the digital world has broader and quicker reach. It is usually the area where children, although being considered as a vulnerable group, are proved to be perpetrators.

In case of perpetrators, one expects a proper fair trial and corresponding punishment. However, if children are included, the minimum age for criminal responsibility of children must be examined. Since there is no consensus among European countries on the minimum age of criminal responsibility of a child, each state has set up its minimum.[70] As for Slovakia, the Criminal Code of the Slovak Republic establishes the age as 14.[71] It means that whatever a child under 14 does, he or she cannot be held criminally responsible. The criminal responsibility of children considers the ability of children to bear consequences of their behavior and has been reduced in Slovakia to the age of 14

66 Another threat lies in misuse of personal data of children provided online by parents by higher risk of personal identity theft or financial fraud. See e.g., UK bank research. https://www.bbc.com/news/education-44153754.

67 See e.g., Art. 16, 18, para. 1 of the Convention on the Right of a Child.

68 Steinberg, 2017, p. 865; see also Stuart, 2014, p. 465.

69 Art. 16 of the Convention on the Right of a Child.

70 See the list of the minimum age for criminal responsibility: https://archive.crin.org/en/home/ages/europe.html.

71 Act no. 300/2005 Coll. Criminal Code, para. 22.

after recodification of the Criminal Code. If a child commits an act which otherwise would be defined as a crime and is not because of his or her age, s/he is not criminally responsible. If over 12, though, s/he might be given protective supervision.[72]

Criminal responsibility includes recognition and control elements. If they miss, the age limit is legally comparable to the state of insanity.[73] Nevertheless, children of today get matured sooner than before on both, the physical and mental levels, rapid technological development might have influenced this phenomenon as well. It is a usual situation that from the technological point of view, children are best to assist their parents.[74] On the other hand, threats of the functioning of the digital world are better known by parents because of their life experience.

The Slovak legal order has finally addressed the issue of cyberbullying. It has been several years since the Criminal Code allowed criminal prosecution of *de facto* cyberbullying by the *de iure* prosecution of several other already defined crimes. *De facto* cyberbullying has been prosecuted by cyberstalking, blackmail, coercion, sexual abuse, defamation, violation of others" rights, child pornography (production, distribution, possession), endangering morality, endangering the moral upbringing of young people, even by prosecution of the crime of the support and promotion of groups working to suppress fundamental rights and freedoms, crime of the production, dissemination and preservation of extremist material, crime of the denial and approval of the Holocaust and crimes of political regimes, crime of defamation of nations, races and beliefs, crime of incitement to national, racial and ethnic hatred, and crime of incitement, defamation, and threats to persons based on their race, nation, nationality, color, ethnic group, or origin.[75]

Nevertheless, the substance of bullying differs from the aforementioned crimes. The aim of bullying is to humiliate or even exclude an individual from a particular social environment. Nevertheless, although the aim of cyberbullying is the same as in the case of bullying, cyberbullying is even more invasive than "traditional" bullying.

First, there is no time or space limitation. So-called traditional bullying is usually limited to one space, e.g., school or work; nevertheless, in the case of cyberbullying, attacks with an aim to humiliate can come anytime and anywhere, the only barrier is a no mobile or no Internet access. Furthermore, its spread is much quicker and broader. It does not affect only those present, not only it can quickly reach a large amount of people, but its distribution is uncontrollable. Another difference is related to anonymity. Perpetrators can feel safer and even less aware of what their behavior causes because they do not see the victim's reaction, they miss the possibility of human empathy that is missing especially in case of social or psychological pathology. Moreover, for the victim, the anonymity of the perpetrator contributes to even greater

72 Ivor, Polák and Záhora, 2021, p. 144.
73 Ibid.
74 Children are considered to be digital natives, see e.g., Kurucová, 2018, pp. 127–135.
75 For the definitions of these crimes, see the Criminal Code. As for the list, https://www.kybersikanovanie.sk/index.php/legislativa.

suspicion, uncertainty, and fear since there might be cases when s/he does not know who to defend against, s/he does not know where the next attack will come from since the perpetrator can be anyone. Finally, cyberbullying overcomes differences more easily, because of anonymity and the use of technical means, it is easier for perpetrators to attack someone they would not have dared to in the real world because of their authority or position. It means that even adults might become a victim of cyberbullying by children. Finally, unlike traditional bullying, the perpetrator and the victim are not in direct contact, so after cyberbullying there are no visible traces of physical harm although physical harm might be even more serious.[76]

Considering all these differences, one admits the special danger of cyberbullying that must be dealt with by special means of criminal law. It is one of the effective ways how a state might fulfill its positive obligation under Art. 8 of the Convention. Because of a criminal principle of *nullum crimen sine lege*, a new crime had to get defined to allow police and other law enforcement authorities to prosecute cyberbullying. It was done so by an amendment of the Criminal Code in 2021 when a new crime was incorporated into the Criminal Code, namely the crime of dangerous electronic harassment. As it has already been, the crime of cyberbullying is specific because of the intent to humiliate a victim. It is one of the features that must be met if a person is to be prosecuted for this crime.

To analyze this important step of right to privacy protection under Slovak framework requires a precise definition:

> Who intentionally degrades the quality of life of another by means of an electronic communications service, computer system or computer network by:
> (a) degrading, intimidating, acting on his/her behalf or otherwise harassing him/her[77] on a long-term basis; or
> b) unjustifiably publishing or making available to a third party a visual, audio, or audio-visual recording of his/her personal presentation obtained with his/her consent, capable of significantly jeopardizing his/her seriousness or causing him/her other serious harm to his/her rights,
> will be punished by imprisonment for up to three years. [78]

To sum up definitional elements of the new crime, there must be: the intent, longevity, degradation, intimidation, harassment, or serious harm to the rights of a victim, and finally, a significant deterioration in the victim's quality of life.

Although a part of the definition of the new crime, there is no additional definition of the degradation or intimidation. Consequently, keeping in mind the Court's

76 Compare https://www.zodpovedne.sk/index.php/sk/ohrozenia/kybersikanovanie.

77 Slovak language distinguishes three linguistic genres: male, female, neutral. Within legal text, male version of "who" and "other" is used, "her" has been added preventively here by the author to make sure that no one is excluded within understanding of a reader.

78 Para. 360b of the Criminal Code.

explanation,[79] definitions used in the Convention's interpretation by the ECtHR should be used. Therefore, treatment that is intended to humiliate or debase an individual, showing a lack of respect for or diminishing their human dignity, or arouses feelings of fear, anguish, or inferiority capable of breaking an individual's moral and physical resistance, is considered degrading.[80] Furthermore, behavior can be considered intimidating when the aggressor arouses fear or apprehension in the victim that certain harm will occur on his/her side, regardless of whether that harm is to occur immediately or to be inflicted later.[81]

When preparing the amendment, it was expected that the explicit regulation of the specific crime of dangerous electronic harassment will undoubtedly facilitate the derivation of responsibility for aggression through communication services and social networks. Nevertheless, as usually, practical application means unexpected challenges as proved in the following example.

Slovakia was shocked by an incident that took place in Miloslavov, a town in the western part of the Slovak Republic. Several children, aged 14, 15, and 16, assaulted an 11-year-old girl by beating her, getting her drunk, and after undressing her, they recorded her and published the video on social media.[82] Immediate response from all the authorities responsible for children took place, including psychologists *in situ*. Nevertheless, questions have remained concerning punishment.

There were allegedly 10 perpetrators present at the place of the attack, one of whom was younger than 14 and therefore could not be held responsible. All the other attackers were expected to be prosecuted for several crimes, those who had published videos online and participated in their dissemination, especially for cyberbullying. However, the situation has been proved to be more complicated since the newly adopted amendment of the Criminal Code on cyberbullying is not applicable.

There is no doubt that the trauma suffered by the 11-year-old girl is doubled. First, the brutality of the attack has fundamentally violated her right to inviolability of a person under Art. 16 of the Constitution. Second, videos of the assault quickly began to spread on the Internet. Although the investigation is still ongoing,[83] so far only the attack itself can be prosecuted, not the dissemination of videos that were recorded and later published. The problem is the element of consent in the new crime of dangerous electronic harassment. It only applies to videos that were acquired with the consent of the person but have been published without their consent. The video under investigation has been recorded without the consent of the assaulted girl.

As for this current case, "only" traditionally used crimes are available to be prosecuted, such as aforementioned crimes of defamation, violation of others' rights, child pornography (production, distribution, possession), endangering morality,

79 See e.g., Constitutional Court, PL. ÚS 5/93 from 18 May 1994, decision, pp. 10 et seq.
80 See e.g., ECtHR, *M.S.S.* v. Greece and Belgium, 2011, no. 30696/09, para. 220.
81 Compare Ibid.
82 See e.g., https://www.zenyvmeste.sk/miloslavov-dievca-napadnutie-kamarati-sikana.
83 This part of the chapter is being written in April 2022.

endangering the moral upbringing of young people. The police have already informed that the leader of the group is accused of the crime of injury to health and the crime of rioting.[84] This 16-year-old girl faces half the sentence compared to the situation if she committed the same crime as an adult.

Nevertheless, as for the possible applicability of the new crime to similar situation *pro futuro*, another amendment of the Criminal Code should be adopted that would concern consent. It is a clear demand for proper and effective protection of the right to privacy. Bullying is becoming increasingly common in the online space and has been proven to be a huge problem despite all kinds of national plans and other ways of criminal prosecution as mentioned above. The new wording of the crime should therefore also deal with finger-pointing, intimidation, humiliation, or sharing of private photos and videos via the Internet, especially in the cases in which the victim did not give consent.

Bullying most often occurs in the real world. From here, conflicts are also transferred to the digital world. It follows that the prevention of cyberbullying is to develop relationships, to work on solving conflicts and to increase the ability to empathize with the experiences of others.[85] Having said that the cyberbullying has been the case when children are often seen as perpetrators, it is very important to point out that cyberbullying is present also among adults. Specific regulations must have been adopted to prevent right to privacy violation e.g., in case of employees.

## 5. Right to privacy and unauthorized monitoring

Even if not at the level of bullying, the right to privacy might be violated also by other means, such as monitoring.

Right to privacy in general is protected by Art. 16 of the Constitution and broadened by *lex specialis* within Art. 19 of the Constitution and Art. 22 of the Constitution. The former concerns protection against unauthorized collection, publication, or other misuse of personal data,[86] the latter focuses on protection of personal data as such.[87] Although the subject of the protection is the same, personal data, they

84 Information provided by police in their Facebook status. https://www.facebook.com/KRPZBA/photos/a.604815706607630/1373949529694240/?type=3.

85 See further recommendations: https://www.zodpovedne.sk/index.php/sk/ohrozenia/kybersikanovanie.

86 See Art. 19, para. 3 of the Constitution.

87 See Art. 22 of the Convention: "(1) The privacy of letters and secrecy of mailed messages and other written documents and the protection of personal data is guaranteed. (2) No one may violate the privacy of letters and the secrecy of other written documents and records, whether they are kept in privacy, or sent by mail or in any other way, except for cases which shall be laid down by law. Equally guaranteed is the secrecy of messages conveyed by telephone, telegraph, or other similar means.".

pursue a different goal, as if Art. 22 of the Convention was *lex specialis* in relation to Art. 19 of the Convention since it guarantees protection against secret surveillance of communication.

Nevertheless,

> by limiting the protection of personal data to protection against unauthorized processing of personal data, the Constitution implicitly allows for the legitimate processing of personal data. The Constitution does not preclude any collection of personal data.
> Protection is granted only against unauthorized collection, disclosure, or other misuse of data. Legally collected data must be stored by a public authority in such a way that they are protected from unauthorized access by other public authorities, including natural and legal persons. If a public authority collects data on a person who is not entitled to identify, store, or otherwise obtain in its disposal sphere, it shall commit conduct inconsistent with Art. 8, para. 2 of the Convention. The state of technology making it difficult to access data or other measures taken to protect the data stored in the information system cannot be confused with the protection against unauthorized collection of personal data.[88]

The relationship between Art. 19 and Art. 22 of the Convention is very important since it has influenced the methodology of examination whether there has been unlawful interference into personal data protection. First, application of Art. 22 of the Convention is analyzed by reviewing whether there has been secret surveillance of personal data. Even if not, use of personal data reviewed under Art. 19 of the Convention follows. It has been so e.g., in case of constitutionality check of some articles of the Act on Electronic Communication.[89] Technological development has enabled various ways of data collection, nevertheless, not everything that is technically possible is legally in accordance with the Constitution although the law may even require it. The amendment of the Act on Electronic Communication has imposed an obligation on electronic communications providers to retain traffic, location, and communicating party data from the date of the communication for six months for Internet connections, Internet e-mails, and Internet telephony, and for twelve months for other types of communication.[90] Although it was not a question of monitoring the content of the communication as such, it is also possible to obtain information of a personal nature within the framework of profiling from the aforementioned information, as has been pointed out by the Court since

> from the above data on users, recipients, exact date, time, and duration of communication, type of communication, data related to terminal identification, or data

88 Constitutional Court, III. ÚS 400/2016 from November 29, 2016, finding, p. 7.
89 See Constitutional Court, PL. ÚS 10/2014 from 29 April 2015, finding.
90 Act no. 351/2011 Coll. on Electronic Communications.

> needed to identify the location of a mobile terminal; relatively detailed information on social or political affiliation can be compiled in their mutual combination, as are personal hobbies, health, sexuality, and the inclinations or weaknesses of individuals. From the data that electronic communications providers are obliged to retain, it is also possible to draw sufficient content conclusions that fall within the private sphere of the individual.[91]

Moreover, the

> considerable intensity of the invasion into the right to privacy was also due to the fact that the stored data and their subsequent use without informing the subscriber or registered user might make the persons concerned feel that their private life is subject to constant monitoring.[92]

As soon as the Court finds interference into the private sphere of the individual, it admitted the legitimate aim of crime prevention and protection of public security; however, when applying the test of proportionality, it found it in violation of the constitutional protection of the right to privacy. Not only did the examined regulation apply to all participants and registered users, including those not indirectly involved in a situation that could lead to criminal prosecution, and even those whose communications under the relevant legislation are subject to professional secrecy or to a duty of confidentiality established or recognized by law,[93] "the objective pursued by the contested legislation in supporting the fight against serious crime and, ultimately, public security could also be achieved by other means which constitute a less intensive invasion of the right to privacy."[94] The Court noted other tools that it considered more appropriate than the widespread and preventive retention of the relevant data, such as the so-called data freezing, which after meeting the specified conditions, is allowed to monitor and store the necessary and selected data only with a specific, predetermined participant in the communication.[95] Moreover, the Court also objected to insufficient safeguards and means of protection for the individuals concerned to effectively protect personal data against the risks of leaks, misuse, or any illegal access or illegal use of this data.[96]

Although there is a legal definition of personal data as

> data relating to an identified natural person or an identifiable natural person which can be identified directly or indirectly, in particular by a generally applicable identifier, another identifier such as name, surname, identification number, location data,

91 See Constitutional Court, PL. ÚS 10/2014 from 29 April 2015, finding, para. 106.
92 Ibid. para. 107.
93 Ibid. para. 120.
94 Ibid. para. 122.
95 Ibid.
96 Ibid.

> or an online identifier, or based on one or more of the characteristics or traits that make up its physical identity, physiological identity, genetic identity, mental identity, mental identity, economic identity, cultural identity or social identity,[97]

the Constitution provides protection also for legal persons. Furthermore, not only data collection itself, but also the way how the data are collected is important. Monitoring of a public space and not intentional or intentional data collection in such a case even if a person is not aware of it is not violation of the right to privacy according to Art. 19 neither Art. 22 of the Constitution if it done on a legal basis.[98] However, there might be a problem with use of the data if collected systematically and intentionally. Furthermore, special protection is provided to the communication between an advocate and his or her client.[99]

Although several years ago, *Kvasnica* (decided by the ECtHR) is a perfect example of not only secrecy surveillance problem but also of leaking information including personal data from official bodies.[100] This case was selected not only because of the ECtHR decision but also because of a rather often situation also in the current Slovak media attitude to online publication of information not supposed to be shared

97 Act no. 18/2018 Coll. on Personal Data Protection, para. 2.

98 Orosz and Svák, 2021, p. 246.

99 Communication between an advocate and a client is included also in documents that are especially protected. Nevertheless, they might be sometimes seized. Since the amount might be huge in electronic version, specific rule is to be observed. As the Constitutional Court in its decision no. II. ÚS 96/2010 from February 3, 2011, p. 32, observes, "Digital world and related technological development have enabled various forms of data collection, including for the purposes of criminal investigation, such as complete data extraction from notebooks, mobiles, or other data carrier, including those that are not relevant for a particular criminal case. The question is therefore appropriate what the balance between interference into the right to privacy and necessity is to conduct effective criminal investigation when huge amount of data need much time to get examined to select the relevant part. The Court has been consistent by pointing out the Criminal Procedure Code whose systematic interpretation allows isolation of data relevant to criminal proceedings and subsequent disposal of a copy containing the complete set of data recorded on the storage medium, or its return to the relevant individual." The Court has thus applied existing legal rules appropriately what has been confirmed in its decision no. IV. ÚS 210/2020 from May 26, 2020, paragraph 66, in which it has elaborated the time element and proportionality principle and decided that "data extraction without prior selection is constitutionally acceptable form of execution of the order for storage and issuance of computer data. Lengthy analysis of data on various material carriers in the place where the house search is performed, respectively inspection of other premises, for the purpose of extraction of only selected data, or removal of material carriers themselves and subsequent thorough data selection and extraction and copying of only selected data represent a much more invasive intervention compared to surface data extraction without their previous selection. After such surface extraction, the procedure according to §90 para. 3 of the Criminal Procedure Code, which allows the interpretation that this procedure may also be applied to a part of the computer data obtained, i.e., if a certain part of the data is reliably established by selection and analysis, that they are not necessary for the purposes of criminal proceedings, e.g. because they have nothing to do with the matter, the order to cancel the retention of this data may be applied to the specified group of data, depending on the specific circumstances, it is not necessary to wait for the selection of the entire volume of data.".

100 ECtHR, *Kvasnica* v. Slovak Republic, application no. 72094/01, June 9, 2009.

because of being a part of criminal prosecution.[101] Moreover, as with the *Kvasnica* case, even in the current Slovak public space, there has been a conflict within security forces that is partially realized by having information leaked.[102]

As for the facts of the *Kvasnica* case, the complainant was a lawyer, an active advocate at the time. Between August 1999 and March 2001, he acted as a lawyer for several industrial companies belonging to the group associated with strategic steel mills in eastern Slovakia, and from April 18, 2001, he was on the board of directors of the company that owned the factory. In 1999, the Minister of the Interior set up a specialized investigation team to clarify the extensive organized criminal offenses of a financial nature which were committed in connection with a company belonging to the above group.

The investigators asked the court to consent to the interception of the applicant's telephone, and the judge of the Regional Court in Bratislava granted the request. Subsequently, calls from and to the complainant's mobile phone were intercepted.

In November 2000, the applicant learned that calls from his telephone had been recorded, that the interception was carried out by the financial police, and that the content of his telephone communication was known outside police environment. On January 5, 2001, the applicant received an anonymous letter confirming the above information and stating that the interception took place from October to December 2000, upon request of opponents of his clients. On May 31, 2001, and June 1, 2001, a newspaper published an interview with the Minister for the Interior and the head of the president's police force. From the content of these interviews, the complainant understood that they confirmed that his interception had taken place. Moreover, transcripts of the applicant's interviews leaked and were made available to various interest groups, politicians, and journalists as well as representatives of several legal entities.

In the summer of 2002, the applicant was informed that transcripts of his interviews with third parties recorded by financial police are freely available on the Internet. These transcripts included his interviews with colleagues, clients, representatives of the other party to the proceedings and friends. The transcripts have been amended to include statements which the complainant and the other persons concerned did not make.

Not only the applicant but also the director of the special division of the financial and criminal police lodged a complaint based on violation of relevant domestic legal norms. Nevertheless, the judge who had authorized the interception made a written statement to the president of the regional court stating that the request for the authorization had met all formal and substantive requirements. He admitted though that

101 There is a conflict between a right of public to information (usual media claim) with a right to a fair trial (usual lawyers and their clients claim). Nevertheless, such a conflict (especially in relation to the principle of proportionality) should be decided by an independent court, not by public mood. See e.g., https://zurnal.pravda.sk/neznama-historia/clanok/607289-pozor-na-uniky-informacii/.

102 See e.g., https://spravy.rtvs.sk/2021/06/inspekcia-ministerstva-vnutra-zasahovala-v-naka-k-zasahusa-vyjadril-aj-minister/.

requests for authorization were made in writing but were submitted in person and that oral presentation was usually more comprehensive than the written request. Moreover, he pointed out that judges had to rely on the information in the request for authorization, which presupposed a certain level of trust.

Although there were other complaints submitted by the applicant, no information about the investigation's result was served on him. He even submitted criminal complaints, but they were all rejected, apart from one that was started by a police officer who was later asked to leave the police force for not respecting a general order within the police corps to reject all of the applicant's complaints. Finally, the government submitted a position paper of the general prosecutor which stated that all decisions had been taken in accordance with the law.

Since the complainant did not exhaust all effective domestic remedies (specifically a complaint possible under Civil Code, Art. 13), the ECtHR declared inadmissible his complaint about interference resulting from the copying, misuse, distribution, and publication of the transcripts of his telephone conversations. Nevertheless, as for the interception itself, it found that Art. 8 of the Convention was violated for several reasons. First, according to the ECtHR, it has not been shown that the guarantees relating to the duration of the interference were met, whether there had been judicial control of the interception on a continuous basis, whether the reasons for the use of the devices remained valid, and whether in practice measures were taken to prevent the interception of telephone calls between the applicant as a lawyer and criminal defendants as his clients. Moreover, the ECtHR found that it had not been shown that the interference restricted the inviolability of applicant's home, the privacy of his correspondence, and the privacy of information communicated only to an extent that was indispensable and that the information thus obtained was used exclusively for attaining the aim set out by law. Furthermore, statements by several police officers and the judge involved were indicative of several shortcomings regarding compliance with the relevant law in the applicant's case. In particular, the director of the special division of the financial and criminal police had concluded that the interference at issue had not been based on any specific suspicion against the applicant and no specific purpose had been indicated in the relevant request. In addition, as it has already been indicated, the judge who had authorized the interception remarked that similar requests were made in writing but were submitted by the police investigators in person, which made the request more comprehensive. Finally, there was the information involved that the request for authorization of the interception of the applicant's telephone had been drafted without a prior consultation of the case file and the documents before the Court contained no information indicating that those statements were unsubstantiated.[103]

Apart from this specific problem with unauthorized interception within criminal matters, there has been special legal area that concern much more people in their

103 Ibid. paras. 86, 87.

ordinary working lives, namely legal regulation of a relationship between an employee and an employer.

It is true that the Labor Code does not contain a comprehensive legal regulation concerning the protection of the personality of a natural person, including his or her right to privacy as the Civil Code does. However, some selected provisions of the Labor Code are, in essence, aimed at the protection of individual personal rights such as the right to privacy or the right to the protection of the health and life of a natural person. Nevertheless, when assessing the protection of the employee's personality in an employment relationship, attention should be paid to the possibility of applying the above provisions of the Civil Code first and subsequently to individual provisions of the Labor Code according to which "unless this Act provides otherwise in the first part, the general provisions of the Civil Code shall apply."[104]

In addition to the protection under the Convention and the Civil Code, there are several provisions of the Labor Code that are aimed at the protection of employees and their privacy. As far as the control of employees by the employer is concerned, i.e., by monitoring in a form of the collection of information, it is possible to speak of an interference with the personal life of the employee. Pursuant to Art. 11, which forms one of the basic principles laid down by the Labor Code, the employer may only collect personal data about the employee related to the employee's qualifications and professional experience and data that may be relevant to the work the employee is to perform, perform or has performed.

A distinction must be made between the collection of information and data by the employer before and after the employment of the employee. As for the former, Art. 41 of the Labor Code regulates the relations between the employer and the employee. First, in a positive way when it indicates what the employer may request from the natural person applying for the job, i.e., only information that is related to the work s/he is to perform.[105] The employer may require a natural person who has already been employed to submit a work report and a certificate of employment. Second, in a negative way when it defines data that the employer cannot request from a natural person, such as information on pregnancy,[106] family circumstances, or political affiliation, trade union membership, or religious affiliation.[107]

If the employment relationship has been established, the employer has a different position in obtaining information about the employee.

In accordance with the general principles of legality, legitimacy and proportionality, employee monitoring will be lawful only if such control is required by law and will be carried out only to the extent and to the extent provided by law. Monitoring of employees is legitimate only if the employer fulfills its obligation to notify

104 Act no. 311/2001 Coll. Labor Code, Art. 4 para. 1.

105 See Art. 41, para. 5 of the Labor Code.

106 However, pursuant to Art. 40, para. 6 of the Labor Code, only an employee who has informed the employer in writing about the pregnancy is considered a pregnant woman. Fulfillment of the information obligation is conditional on its special legal protection.

107 See Art. 41, para. 6 of the Labor Code.

the employee and notifies him or her in advance of the existence of the inspection, the scope of the inspection and the form and manner of the inspection. The principle of proportionality will be respected if the inspection is carried out only to the extent necessary, for example to respect occupational health and does not infringe the human dignity of the employee.

Keeping in mind technological development and technological monitoring possibilities, it must be pointed out that as it has already been referred to, Act on personal data protection defines what personal data are, however it provides only a demonstrative calculation. Therefore, the IP address of the Internet connection being used might be considered personal data as well.

To indicate expressly stated legal protection, according to Art. 13 para. 4 of the Labor Code, the employer may not infringe the employee's privacy at the workplace and in the employer's common premises without serious reasons due to the special nature of the employer's activities by monitoring him, recording telephone calls made by the employer's technical work equipment and checking e-mail sent from the work e-mail address and delivered to this address without notifying him in advance. If the employer implements a control mechanism, he is obliged to discuss with the employees' representatives the scope of the inspection, the method of its implementation, as well as its duration and inform the employees about the scope of the inspection, the manner of its implementation and its duration. To be more specific, serious reasons, as defined in that provision, must in each case be assessed individually, depending on the nature of the work, the place of work and the like.

The overall protection by the Labor Code therefore allows the employer to control the work activities of its employees, but s/he must choose appropriate means and forms that do not conflict with the legislation protecting the employee's privacy. For example, the camera system can be used by the employer, provided that the protection of the employee's privacy is not infringed and if the purpose pursued by the employer cannot be achieved otherwise. The aim of the employer might be also control compliance with the working rules, however, the employee must be informed by the employer about the camera monitoring, namely its scope, time duration and the manner of its implementation.

As regards the monitoring of electronic mail, in accordance with the mentioned Art. 13 para. 4 of the Labor Code, the employer may not, without serious reasons based on the special nature of the employer's activities, infringe the employee's privacy at the workplace and in the employer's common premises, by checking e-mail sent from and delivered to the work e-mail address unless warned in advance.

Those serious reasons in such a case also must be assessed individually in the case of e-mail tracking about the subject and activity of the employer, for example the protection of the employer's intangible assets, such as trade secrets. Nevertheless, before the employer carries out the employee's e-mail check, he or she must present those serious reasons and inform the employee about the scope, method, and duration of the e-mail check.

Nevertheless, if the employee considers that the monitoring is illegal and his or her private life or personality rights have been violated, s/he has the right to submit a complaint to the employer who is obliged to respond to the employee's complaint without undue delay, to make a correction, to refrain from such action and to eliminate its consequences.[108]

The employer may regulate in its internal regulations the use of electronic mail by employees. When using Internet access and e-mail services, the employee is obliged to comply with applicable laws and internal regulations of the employer, which may include various restrictions, such as the use of e-mail not violating the job's rules or activities that conflict with and unrelated to the employer's business. On the other hand, an employer may allow an employee to use e-mail and Internet access for any private purposes.

As for monitoring of telephone calls, it might be exercised to prevent employees to use a work telephone for private purposes. Nevertheless, privacy must be observed when monitoring telephone calls, it means that the content of telephone calls must remain confidential, the employer can only check called numbers.

The employee's liability arises when s/he commits an illegal act or a breach of duty, a breach of work discipline consisting e.g., in the use of official equipment for private purposes.

Personal inspection of the employee by the employer can also be understood as monitoring of the employee: its purpose in practice lies in the prevention of removal of inappropriate things to and from the workplace.[109] More detailed conditions must be determined by the employer in the working rules, first, personal inspection must be carried out at the workplace and during working hours, otherwise the employee's right to privacy would be violated. Moreover, protection of personal liberty must be observed during the inspection and human dignity must not be degraded.

## 6. Right to privacy and unauthorized registration of personal data

Apart of monitoring, two specific cases have been selected to be analyzed in relation to the issue of the right to privacy within data collection and processing. The first was decided by the ECtHR and is related to the violation of Art. 8 of the Convention. The second was decided by the Court of Justice and was based on an analysis of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and on the right to privacy protection in relation to processing of personal data laid down in Directive 95/46/EC (1) of the European Parliament and of the

108 Compare Art. 13, para. 6 of the Labor Code.
109 Ibid. Art. 177, para. 2.

Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

As for the first one, it deals with specific situation referring to existence of so-called StB files and registration within them. During the Communist regime, the State Security Service (Štátna bezpečnosť, or StB) held its files with lists of collaborators. Those collaborators were divided into several groups based on the level of their cooperation, such as agents or candidates for cooperation or informant.[110] After the fall of the Communist regime, those StB files were made available (although some were destroyed) and several people realized they were within the lists without giving their consent to cooperation.

There were several cases decided by both supreme courts of the Slovak republic, some of them dealing with the issue of passively legitimacy of an entity in proceedings for the protection of the personality of a natural person registered in the StB files, i.e., who is responsible for interference into personality rights.[111] At the beginning, it was Slovak Intelligence Service that was under the control of Ministry of Inferior that was in charge of administration of the files, later on, this administration duty has been transferred to the Institute of the Memory of the Nation. The Institute is not a state body; nevertheless, in accordance with legal obligations, it was imposed to make all the handed over documents available, to publish all the relevant data and provide the necessary information designated by the public authority.[112] According to the Supreme Court, it has been held at the same time as the entity responsible for the risk associated with these tasks, if the data in these materials, respectively registration in them, is unjustified, even though it has not been expressly so identified in the legal act.[113]

Identifying who is responsible for the unjustified registration and therefore unjustified processing of personal data has taken several years and judicial bodies to get the final decision. The Constitutional Court finally decided upon the status of the Institute and its responsibility in relation to the claimed interference in personality rights of allegedly unjustifiably registered individuals.[114]

According to the Court, the mere fact that a body (a public body) has become *ex lege* the holder of physical media on which the outputs of (official) activities of public authorities are captured does not in itself constitute a transfer of responsibility for the unjustified interference with the right to protection of personality which might have taken place.

The Court has pointed out that the general courts appear to have relied on the considerations set out in one by which passive legitimacy was referred to the Slovak

110 See e.g., website of the Institute of the Memory of the Nation that provides information about several categories of collaborators. https://www.upn.gov.sk/sk/vysvetlivky-k-registracnym-protokolom/.

111 See e.g., Supreme Court of the Slovak Republic, 6 Cdo 83/2010, decision from 31 May 2011.

112 Act no. 553/2002 Coll. on the Institute of the Memory of the Nation.

113 Supreme Court of the Slovak republic, 6 Cdo 83/2010, decision from May 31, 2011, p. 5. See also Supreme Court of the Slovak Republic, 5 Cdo/83/2008 from November 27, 2009.

114 Constitutional Court, II. ÚS 285/2017 from October 12, 2017, finding.

Intelligence Service. However, at that time, the Slovak Intelligence Service was a state body, i.e., a body acting on behalf of the state. Moreover, in that case, it was not a matter of determining the originator of the intervention and the responsible person, as it was not disputed that the originator of the intervention was the state; it was therefore only a matter of designating a state body, which has passive legitimacy.[115] However, the Institute is not a state body and therefore the relationship between the persons registered in the StB files and the public authority clearly cannot be described as private, and therefore no personality protection based on Civil Code applies to them.[116]

In addition, the Court has analyzed a possible reasoning that it was not the registration but the publication of the files that interfered with the individual's rights within the meaning of Art. 13 of the Civil Code, i.e., by the act of publishing an already existing information or document. It means that although individual allegedly did not cooperate, the information claiming the opposite has been published without having been proved. The Court has not ruled out in general terms that an intervention within the meaning of Art. 13 of the Civil Code may also consist in the publication of information obtained by a state authority in the performance of its statutory tasks. In this context, however, Art. 13, para. 1 of the Civil Code explicitly provides protection (only) against unauthorized interference.[117]

The Act on the Institute of the Memory of the Nation established the public constitution (as well as other public institutions), and empowered it to perform tasks of a public nature, in this case related to dealing with the past. Art. 19 para. 1 of this Act stipulates the obligation of the Institute to publish in print and on electronic media a transcript of records from preserved or reconstructed files. The Court has repeatedly emphasized that the Institute has no discretion in publishing registration protocols, i.e., the right to decide whether to publish a part of them. The Institute does not even rewrite the data in these protocols (where a transcript might be erroneous). The Institute's liability for examining the correctness of the materials entrusted to it is expressly excluded by Art. 26, para. 3 of the specified Act on the Memory of the Nation, according to which "the Institute is not obliged to verify whether the data contained in the document and the data obtained in the information system of documents from the preserved records referred to in paragraph 2 are accurate or true." Fulfillment of this legal obligation is therefore precluded, and by fulfilling it, the Institute acted unlawfully, i.e., that such disclosure (if made exactly in accordance with Art. 19 and other provisions of the Act on the Memory of the Nation) may constitute unjustified interference within the meaning of Art. 13, para. 1 of the Civil Code.[118]

115 Ibid. paras. 28, 29.
116 Ibid.
117 Ibid. paras. 32 et seq.
118 Ibid. paras. 32, 33.

Nevertheless, there have been cases when individuals asked to be deleted from the StB registration files—some of them successful.[119] However, in the selected case, Mr. Turek has had to face more challenging rules.[120]

Mr. Turek worked in the state administration of the school system. He occupied a leading post that fell within the purview of the Lustration Act,[121] which defined some supplementary requirements for holding certain posts in public administration. In January 1992, the applicant's employer asked for a clearance concerning the applicant and received a negative one. It meant that the applicant was disqualified from holding certain posts in public administration, so he resigned from his post, later he left his employer completely, having felt compelled to do so. The information about who was registered in the StB files has been made public in newspapers and online. In May 1992, the applicant lodged an action for protection of his good name and reputation; he alleged that his registration as a collaborator was wrongful and unjustified.

The applicant admitted having met StB agents several times before and after his journeys abroad, when they had instructed him on how to behave abroad and asked for information about his stay. Nevertheless, according to the applicant, their discussions were of a general nature and included the situation at the applicant's workplace. The applicant admitted having obtained and provided a list of students who had been preparing for studies abroad; however, he considered information public in any case. He had never had the impression that he was considered a collaborator and had never been asked to keep his contacts with StB officers' secrets.[122]

The lower national courts established that the applicant's meetings with StB agents amounted to formal collaboration, and that the applicant had failed to prove that that his registration as a collaborator had been contrary to the rules applicable at the material time. Moreover, the Supreme Court held that the fact that the applicant was registered in the StB files did not by any means constitute evidence that he had been a conscious collaborator of the StB. In addition, in line with established judicial practice, the Supreme Court noted that the procedure concerning the issuance of a security clearance under the Lustration Act could not amount to a violation of an individual's good name and reputation, since only unjustified registration in the StB files would amount to such a violation. The Supreme Court considered that it was crucial for the applicant to prove that his registration had been contrary to the rules applicable at the material time and concurred with the lower courts' conclusions that the applicant had failed to do so.[123]

119 These were cases when an individual had to prove that the official registration information was fabricated already at the time it was done, e.g., by including fake information by the police agents themselves. See e.g., a story of František Krajňák, 2014. https://zivot.pluska.sk/pribehy/knaz-frantisek-krajnak-ocistil-svoje-meno-nebol-agentom-stb. However, as it is pointed out in the article, as a result, even if there was a judgment of the Court, the name is not deleted from the list, the Institute only upload the judgment on its website. On the contrary, if a claimant is successful in the Czech Republic, his or her name is deleted from the registration file.

120 ECtHR, *Turek* v. Slovakia, no. 57986/00, February 14, 2006.

121 Act no. 451/1991 Coll. Lustration Act.

122 ECtHR, *Turek v. Slovakia,* no. 57986/00, February 14, 2006, para. 48.

123 Ibid. para. 57.

As for the ECtHR proceedings, the most important argument in relation to the alleged violation of Art. 8 of the Convention was the applicant's claim that during the lustration proceedings, he had been denied access to guidelines that defined the category of "agent" and established rules of cooperation with agents, since the document was classified "top secret."

The ECtHR did not follow the Supreme Court's decision about non-violation of an individual's good name and reputation, it observed that the applicant's registration as a StB collaborator affected his name and reputation and therefore interfered with the requirements of Art. 8 of the Convention. The ECtHR then decided whether the interference was justified, examining whether the procedural protection at the domestic level of the right of Mr. Turek to respect his private life was "practical and effective." The Court acknowledged that there may be legitimate grounds to limit access to certain documents and other materials. However, the Court concluded that denial of access to the requested information in the circumstances of the instant case was unnecessary for three reasons.

First, the Court stated that the nature of lustration proceedings indicates that they are oriented towards the establishment of facts dating back to the Communist era, and they are not directly linked to the current functions and operations of the security services. Thus, "it cannot be assumed that there remains a continuing and actual public interest in imposing limitations on access to materials classified as confidential under former regimes."[124] Secondly, due to the nature of the lustration proceedings, if the applicant to whom classified material relates is "denied access to all or most of the materials in question, his or her possibilities to contradict the security agency's version of the facts would be severely curtailed."[125] Finally, since the respondent in the lustration proceedings is the security agency, which has the power to decide what materials should remain classified and for how long, "This power is not consistent with the fairness of the proceedings, including the principle of equality of arms."[126] The Court therefore concluded that the domestic courts placed an unrealistic burden on the applicant, since he was required to prove that his designation as a collaborator was unjustified without having access to the applicable rules, while the state did have full access.[127]

Another very specific case dealing with the right to privacy protection because of alleged unlawful or unjustified registration of an individual concerns a case decided by the Court of Justice. It had been decided before the GDPR adoption, therefore based on the analysis of the Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and also on the analysis of the Charter of Fundamental Rights of the European Union, Arts. 7 (protection of the right to respect for private and family life, home and communications), 8 (protection of the right to the

124 Ibid. para. 115.
125 Ibid.
126 Ibid.
127 See also the summary. https://globalfreedomofexpression.columbia.edu/cases/turek-v-slovakia/.

protection of personal data), and 47 (protection of the right to the effective remedy). In the decision, the Court of Justice had to deal with a request for a preliminary ruling from the Supreme Court of the Slovak Republic. The case concerned a dispute between Mr. Peter Puškár and the Finance Directorate of the Slovak Republic and the Criminal Financial Administration Office upon a list of persons considered by the Finance Directorate to be the so-called "white horses," i.e., people to whom a legal entity is assigned, in which the white horse is "active" with the birth number of the white horse, the tax identification number of the tax entity in which the white horse is active, and the "functional" period of the white horse.[128] White horses are persons who only lend their first and last name and their identity to assume rights and obligations that they have no real interest in exercising. This concept is used unofficially to identify individuals that are usually misused by third persons to exercise unfair exercises. The mentioned applicant asked in the case for an order requiring those authorities to remove his name from the list created in the context of tax administration. The Court of Justice was asked four preliminary questions, one of which is relevant for the research area.[129]

The basis of the question lies in the interpretation of the directive and Art. 7 and Art. 8 of the Charter in relation to the legal possibility of a Member State to create, without the consent of the person concerned, a register of personal data for the purposes of tax administration, so that the fact that personal data is rendered at the disposal of a public authority for the purposes of countering tax fraud in itself constitutes a risk.

First, the Court of Justice has clarified that the making the list in question constitutes the processing of personal data within the meaning of the Directive and therefore falls within the scope of that directive. The Court of Justice has then pointed out that personal data may be lawfully processed "if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority."[130] According to the Court of Justice, the collection of taxes and the fight against tax fraud, for which the disputed list is established, must be regarded as tasks carried out in the public interest, but emphasizes that it is for the Supreme Court to assess whether the Slovak authorities who made the list, or those authorities addressed in the list, were entitled to do so under Slovak legislation. Moreover, apart from the principle of legality, it is for the Supreme Court to determine whether the establishment of the contested list is necessary for the purpose of collecting taxes and combating tax fraud and whether those objectives cannot be achieved by less restrictive means. It therefore means that EU law does not preclude the processing of personal data by the authorities

128 See Supreme Court of the Slovak Republic, decision no. 1Sžz/15/2014 from August 23, 2018, para. 6.

129 See Court of Justice of European Union, judgment from September 27, 2017, case C-73/16. The first referred question dealt with a possibility of a Member State to make exercise of the effective remedy conditional upon exhaustion of administrative complaints, the third one aimed at the il/legally obtained registration by the applicant and the possibility of a Member State to refuse such an illegally obtained evidence, the last one focused on a hypothetical collision of the relevant rights protection between the ECtHR and the Court of Justice interpretation (this question was declared inadmissible).

130 Compare ibid. para. 117.

of a Member State for the purposes of tax administration and the suppression of tax fraud.[131]

## 7. Conclusion

Right to privacy has become a challenge in the digital world. Although there are many definitions of digital world in the literature, for the purposes of this chapter, it has been understood as a globally existing sphere within the information environment whose distinctive and unique character is created by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information through interdependent and interconnected networks that use information and communication technologies.[132] This definition precisely defines that even for the operation of the Internet, we need hardware, software, and data. Moreover, it is clear from this definition that cyberspace also depends on several variables because it is not exclusively about the information itself, but also about the way it is transmitted, whether we perceive it in terms of the need for material components or software. In practice, for example, this means that even if we order the goods online, if we want to have them delivered, we not only order it on some technical equipment, but also have it physically delivered to us, and delivery of goods are tied not to cyberspace, but to real space. Even if we order goods online that are not material in nature, e.g., access to databases, someone had to put the data into the system somewhere, and we have access to it through the media also in real time and space. Therefore, it is problematic to perceive the Internet as an exclusively virtual world that could function without rules.

Although Mark Zuckerberg once stated privacy used to be desirable, but today people want to share, are more open,[133] there are still many areas in which individuals want to maintain their privacy. It is their fundamental right, although they might not always realize how easily they can open it to a worldwide auditorium.

This chapter is a contribution presenting and analyzing selected aspects of the Slovak legal framework in relation to the right to privacy protection in the digital age. Selection criteria have considered challenges of the digital world especially in relation to the quick and broad data processing and challenges that are faced by vulnerable groups or in the areas that are considered sensitive. Therefore, children and their right to protection has been analyzed from the point of view of both, perceiving them as victims and on the other side, possible perpetrators. Comparatively, only from the point of view of possible victims, the issue of un/authorized monitoring of

131 Ibid.
132 Kuehl, 2009, p. 28.
133 See https://www.azquotes.com/quote/1370681.

employees has been analyzed. Finally, because of existing international case law, the un/authorized registration of personal data has been analyzed in relation to right to privacy protection.

The Constitution of the Slovak Republic was adopted on September 1, 1992, and that in relation to its Section II, regulating human rights and protecting fundamental freedoms, there has been no relevant amendment. It means that the regulations of the basic legal act of the state were adopted before the Internet era. Nevertheless, interpretation of the most relevant articles of the Constitution about the right to privacy protection—Arts. 16, 19 and 22—have been an operative tool for effective protection of this right also in the digital sphere. It is so also in relation to the Civil Code and personality rights protection. On the other hand, criminal law must have processed some demands regarding *nullum crimen sine lege* principle and therefore, new crimes have been included into the Criminal Code. Nevertheless, as it has been sadly proved by a particular case study, there are still elements that must be amended in the Criminal Code for the state bodies be able to prosecute non-acceptable online behavior in the form of cyberbullying. Furthermore, as for criminal procedure, existing rules have been adapted to the requirements and specificities of the digital world. To conclude, as for Slovakia in general, traditional means of the right to privacy protection are a preferred tool to deal with challenges of the digital era. However, the area of criminal law is different. Therefore, because of the rule of law, the adoption of a definition of cyberbullying is recommended to be amended *in futuro* so that its criminalization did not depend on the consent of an individual whose audio or audio-visual recording of personal presentation was unjustifiably published or made available to a third party.

It is submitted that since as for the application of legal rules, it has been strictly observed that the basic constitutional principle is to be pursued—that state bodies may act solely based on the Constitution, within its scope, and their actions shall be governed by procedures laid down by law; on the contrary, everyone may do what is not forbidden by a law and no one may be forced to do what the law does not enjoin.[134] It has been proved, as Bill Gates declared, that historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules—not just for governments but for private companies.[135] Finally, it is true that it was difficult to find information. Nevertheless, today, it is difficult to choose among it. One could therefore add that it is important to be aware and respectful of the rules by private individuals as well since you never know to whom you are opening the door to your privacy.

134 Art. 2 of the Constitution of the Slovak Republic
135 See https://www.azquotes.com/quote/1370681.

## Bibliography

BROWNLIE, I. (2013) *Princípy medzinárodného verejného práva*. Bratislava: Eurokódex, s. r. o. a Paneurópska vysoká škola.

DRGONEC, J. (2013) *Sloboda prejavu a sloboda po prejave*. Šamorín: Heuréka.

GARAOVÁ, L. (2020) 'Slovakia' in RIJPMA, J.J. (ed.) *The new EU data protection regime*: setting global standards for the right to personal data protection. Hague: Elevent International Publishing, pp. 525–542.

KUEHL, D.T. (2009) 'From Cyberspace to Cyberpower: Defining the Problem' in: KRAMER, F. D., STARR, S., WENTZ, L. K. (eds.): *Cyberpower and National Security*. Washington D C: National Defense University Press, pp. 24–42.

KURUCOVÁ, Z. (2018) 'Aktivity digitálnych domorodcov na sociálnych sieťach', *Media journal,* 6(2), pp. 127–135.

OROSZ, L., SVÁK, J. (eds.) (2021) *Ústava Slovenskej republiky – komentár. Zväzok I.* Bratislava: Wolters Kluwer.

STEINBERG, S.B. (2017) 'Sharenting: Children´s Privacy in the Age of Social Media', *Emory Law Journal*, 66(839), pp. 839–884.

ŠTEVČEK, M., DULAK, A., BAJÁNKOVÁ, J., FEČÍK, M., SEDLAČKO, F., TOMAŠOVIČ, M. (eds.) (2015) *Občiansky zákonník I., II. § 1–880. Komentár.* Praha: C. H. Beck.

STUART, A.H. (2014) 'Google Search Results: Buried If Not Forgotten', *North Carolina Journal of Law and Technology*, 15(3), pp. 463–517 [Online]. Available at: https://doi.org/10.2139/ssrn.2343398 (Accessed: 11 October 2022).

VRŠANSKÝ, P., VALUCH, J. (eds.) (2016) *Medzinárodné právo verejné. Osobitná časť*. Bratislava: Wolters Kluwer.

Chapter VI

# Privacy and Data Protection in Serbian Law: Challenges in the Digital Environment

Dušan V. Popović

## 1. Introductory remarks

In the Republic of Serbia, as in other jurisdictions, there is no unanimously accepted definition of the privacy, either in legal doctrine or in legislative instruments. The national constitutions, including the Serbian one, usually protect the privacy of individuals by referring to: (1) the inviolability of home; (2) the confidentiality of letters and other means of communication; and (3) the protection of personal data. More extensively defined, the right to privacy may also encompass the freedom of thought, conscience, and religion, in the sense that the citizens do not have the obligation to declare their religious or other beliefs. The omnipresence of the Internet, and in particular social networks, search engines and cloud computing, has led to reducing the right to privacy to the right of personal data protection. Indeed, in the digital world, an individual is often reduced to data. Therefore, protecting one's privacy in the digital context means protecting data relating to an identifiable individual. The concept of personal data encompasses not just names, addresses and identification numbers, but also all data that can be traced back to an individual, such as photos, profiles on social networks or browsing history. Typically, social network websites contain user information such as age, relationship status, income, and information about close family members, as well as registered users' addresses. Many online service providers

Dušan V. Popović (2023) Privacy and Data Protection in Serbian Law: Challenges in the Digital Environment. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 199–234. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_6

store personal data about users so that users do not have to re-enter them each time they access the website, e.g., for online shopping, booking travel, etc. More recently, smart devices connected to the Internet, surveillance cameras, and automated decision-making based on online behavior history has raised privacy concerns across the globe. A recent survey revealed that only 7.5% of Internet users in Serbia believe that their personal data is protected online. Moreover, only 20% of Internet users in Serbia believe that it is even possible to protect privacy in the digital environment.[1]

Given the fact that the Republic of Serbia is a member of the Council of Europe and an EU candidate country, its legal system, including the rules on privacy protection, needs to be aligned to that of the Council of Europe and the European Union. However, with respect to the right to privacy, these two international organizations do not have a fully harmonized approach. Both the European Convention on Human Rights, a Council of Europe instrumen, signed in 1950 (ECHR), and the Charter of Fundamental Rights of the European Union, which was declared in 2000, and came into force in 2009 along with the Treaty of Lisbon (EU Charter), have a provision on privacy.[2] Art. 8 of the ECHR and similarly Art. 7 of the EU Charter provide that everyone has the right to respect for his or her private and family life, home, and communications. Moreover, Art. 8 of the EU Charter specifically addresses the fundamental right to the protection of personal data. Consequently, the EU Charter distinguishes data protection from privacy, and lays down some specific guarantees of personal data protection.[3] At the same time, the European Court of Human Rights (hereinafter, the ECtHR) has applied Art. 8 of the ECHR (covering the right to privacy) to give rise to a right of data protection as well. These legal developments raise the question of whether the right to data protection is only a subset of the right to privacy, or whether it provides additional protection.[4] A number of authors consider that, at least within EU law, data protection has gradually been disconnected from the right to privacy, by being regulated on an ever higher regulatory level and through ever more detailed legal regimes.[5] It seems that the approach of the Serbian legislature is similar to that of the EU, given the fact that the constitutional right to data protection is regulated separately from the right to privacy *stricto sensu*.[6]

The chapter begins with an analysis of the international obligations of the Republic of Serbia in privacy and personal data protection, stemming predominantly from the UN legal instruments, the European Convention on Human Rights and

1 Mitrović, 2020, p. 17.

2 Rights derived from international law are referred to as human rights, while rights derived from domestic constitutional law, as well as from European law, are referred to as fundamental rights.

3 Kokott and Sobotta, 2013, p. 222; Oostven and Irion, 2018, p. 9.

4 Ibid.

5 See for example van der Sloot, 2017, p. 8.

6 Constitution of the Republic of Serbia, Official Journal of the Republic of Serbia 98/2006, Arts. 40–42.

the Stabilization and Association Agreement concluded between the EU and Serbia (Section 2). A brief presentation of the existing legal framework for the protection of right to privacy in the Republic of Serbia follows (Section 3), then the right to privacy is analyzed as a value (Section 4). The right to privacy is undoubtedly a value protected by the Constitution, which leads us to explore the fundamental grounds for protecting the right to privacy (Section 5). The right to privacy, and more specifically the integrity of human person and family life, as well as other rights pertaining to a person, enjoy protection in civil law as well (Section 6). In criminal law, the right to privacy is protected by the Penal Code of the Republic of Serbia, which prescribes several types of criminal offences directly or indirectly related to the breach of privacy (Section 7). In Serbian administrative law, a specific mechanism for the protection of personal data has been established under the auspices of the Commissioner for Information of Public Importance and Personal Data Protection (Section 8). It is expected that further expansion of digital technologies shall require additional legislative efforts, particularly in mass surveillance and protection of children (Section 9). An overall assessment of the Serbian privacy and data protection system has been laid out in the final section of the paper (Section 10).

## 2. International obligations of the Republic of Serbia in privacy and personal data protection

The international obligations of the Republic of Serbia in privacy and personal data protection emanate from the country's membership in the United Nations and the Council of Europe, as well as from its EU candidate status. Under Art. 12 of the Universal Declaration of Human Rights, proclaimed by the United Nations General Assembly in Paris on December 10, 1948, no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honor and reputation. The Federal People's Republic of Yugoslavia was not among the signatories of the Universal Declaration of Human Rights in 1948. Although the Universal Declaration is not a legally binding treaty, it is an expression of the fundamental values which are shared by all members of the international community. Moreover, it has had a profound influence on the development of international human rights law. Some argue that because countries have consistently invoked the Universal Declaration in the past decades, it has become binding as a part of customary international law.[7] In 1971, also under the auspices of the United Nations, the Socialist Federal Republic of Yugoslavia

7 Dimitrijević and Paunović, 1997, pp. 69–71.

ratified the International Covenant on Civil and Political Rights.[8] Under Art. 17 of the International Covenant, no one is to be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor and reputation. The International Covenant also prescribes that everyone has the right to the protection of the law against such interference or attacks.

For most European countries, and for Serbia as well, the membership in the Council of Europe represents the main international pillar for the protection of privacy and personal data. The Republic of Serbia became member of the Council of Europe on April 3, 2003, and ratified the European Convention on Human Rights (formally: Convention for the Protection of Human Rights and Fundamental Freedoms) on March 3, 2004.[9] Under Art. 8 of the ECHR, everyone has the right to respect for his private and family life, his home, and his correspondence. Public authorities should not interfere with the exercise of this right except when such interference is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The Republic of Serbia also ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[10] and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.[11] The Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data, and which seeks to regulate at the same time the transfrontier flow of personal data. On the other hand, the Additional Protocol provides for the setting up of national supervisory authorities responsible for ensuring compliance with laws or regulations adopted in pursuance of the convention, concerning personal data protection and transborder data flows. It also concerns transborder data flows to third countries. Data may only be transferred if the recipient state or international organization is able to afford an adequate level of protection. Finally, the Republic of Serbia ratified the Protocol amending the Convention for the Protection

8 Official Journal of the SFR Yugoslavia 7/71.

9 Law on the ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms, Official Journal of Serbia and Montenegro 9/2003, 5/2005 and 7/2005; Official Journal of the Republic of Serbia 12/2010 and 10/2015.

10 ETS No. 108. Law on ratification of the Convention for the protection of individuals with regard to automatic processing of personal data, Official Journal of the FR Yugoslavia 1/1992; Official Journal of Serbia and Montenegro 11/2005. Law on amendments of the Law on ratification of the Convention for the protection of individuals with regard to automatic processing of personal data, Official Journal of the Republic of Serbia 12/2010.

11 ETS No. 181. Law on ratification of the Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, Official Journal of the Republic of Serbia 98/2008.

of Individuals regarding Automatic Processing of Personal Data[12], which has not yet entered into force.[13]

The Republic of Serbia is a country aspiring to join the European Union. In the process of European integration, Serbia signed the Stabilization and Association Agreement with the EU (hereinafter, the SAA)[14] in 2008.[15] Under Art. 81 of the SAA, dedicated entirely to the personal data protection, Serbia is required to harmonize its legislation concerning personal data protection with EU law and other European and international legislation on privacy upon the entry into force of the SAA. Serbia is also required to establish one or more independent supervisory bodies with sufficient financial and human resources to efficiently monitor and guarantee the enforcement of national personal data protection legislation. Further to this, within the statistical cooperation with the EU, Serbia is required to ensure the confidentiality of individual data.[16] The reason for harmonization of the national legal framework with EU rules on personal data protection is to be found in the preamble of the SAA, in which the parties to the agreement reaffirmed their commitment to respect human rights and the rule of law. One of the aims of the SAA is to support the efforts of Serbia to develop its economic and international cooperation, including through the approximation of its legislation to that of the EU.[17] The respect for democratic principles and human rights as proclaimed in the Universal Declaration of Human Rights and as defined, *inter alia*, in the ECHR form the basis of the domestic and external policies of the parties to the SAA and constitute essential elements of this Agreement.[18] To comply with the requirements of the SAA, Serbia adopted its first modern Law on Protection of Personal Data in 2008, adopted the Strategy for personal data protection in 2010[19] and established an independent supervisory body—the Commissioner for Information of Public Importance and Personal Data in 2009.[20]

12 CETS No. 223. Law on ratification of the Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data, Official Journal of the Republic of Serbia 4/2020.

13 As of February 2022.

14 Stabilization and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Serbia, of the other part, Official Journal of the European Union L 278, 18.10.2013.

15 The SAA entered into force on September 1, 2013.

16 Art. 90 of SAA.

17 Art. 1, para. 2 d) of SAA.

18 Art. 2 of SAA.

19 Official Journal of the Republic of Serbia 58/2010.

20 On November 5, 2004, the National Assembly of the Republic of Serbia adopted the Law on Free Access to Information of Public Importance. The Law established an independent supervisory body—the Commissioner for Information of Public Importance. On 1 January 2009, following the entry into force of the 2008 Law on Personal Data Protection, the tasks related to protection of personal data were included in the Commissioner's scope of work. For a more detailed analysis of the national legal framework see Section 3 of this chapter.

## 3. National legal framework for the privacy and personal data protection

The right to privacy enjoys constitutional protection in Serbian legal system. The Constitution of the Republic of Serbia protects the right to privacy in at least two aspects. First, it protects the inviolability of home. Second, it protects the confidentiality of letters and other means of communication. Further to this, the Constitution enshrines the right to personal data protection.[21] The right to personal data protection and the right to privacy should not be considered identical. There are considerable overlaps in the scope of both rights, but also some areas where their personal and substantive scope diverge.[22]

In line with the trends in comparative law, the Serbian legislature predominantly intervened in personal data protection over the area of "traditional" privacy protection, by means of numerous laws and by-laws. The main piece of legislation currently regulating personal data protection in the Republic of Serbia is the Law on Protection of Personal Data (LPPD),[23] adopted in November 2018 and applicable since August 2019.[24] The 2018 LPPD replaced the previous law, adopted in 2008, which was the first modern legislative act regulating exclusively personal data protection.[25] The main reason for adopting the 2018 LPPD was the need to harmonize the Serbian legal framework with the European Union's General Data Protection Regulation (GDPR).[26] The LPPD applies to the processing of personal data wholly or partly by automated means, as well as to processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Also, the LPPD applies to the processing of personal data performed by a controller or a processor who has its business seat/place of residence in the territory of the Republic of Serbia, within the framework of activities performed in the territory of the Republic of Serbia, regardless of whether the processing takes place in the territory of the Republic of Serbia.

21 Constitution of the Republic of Serbia, Official Journal of the Republic of Serbia 98/2006, Arts. 40–42.

22 See Section 5 of this chapter.

23 Official Journal of the Republic of Serbia 87/2018.

24 The LPPD entered into force on November 21, 2018, but its application started nine months from the date of its entry into force, i.e., on August 21, 2019.

25 Official Journal of the Republic of Serbia 97/08, 104/09, 68/12 and 107/12. The first attempts to regulate personal data protection in Serbia were made in 1998, when the Law on Personal Data Protection was passed (Official Journal of the FR Yugoslavia 24/98 and 26/98). However, that law remained "dead letter," since only a few marginal cases of its enforcement were recorded. For that reason, the year 2008 is acknowledged as the beginning of a modern Serbian data protection law.

26 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L119, 4.5.2016.

Further to the LPPD, the Serbian data protection legislation includes the following by-laws:

(1) Rulebook on the manner of prior review of personal data processing,[27] which governs the procedure for notifying and approval by the relevant authority of intended personal data processing;
(2) Decree on the form for and manner of keeping records of personal data processing,[28] which regulates the form for keeping records of data, personal data processing, and the manner of keeping records of personal data processing;
(3) Rulebook on the form and manner of keeping record of the Data Protection Officer,[29] which defines the form and manner of keeping record of the Data Protection Officers;
(4) Rulebook on the form and manner of keeping internal record of violations of the LPPD and measures undertaken in the course of inspection supervision;[30]
(5) Rulebook on the form of notification on personal data breach and manner of notifying the Commissioner for Information of Public Importance and Protection of Personal Data;[31]
(6) Rulebook on the complaint form,[32] which defines the complaint form that a natural person can submit to the Commissioner if he or she considers that the processing of his or her personal data has been carried out contrary to the provisions of the LPPD;
(7) Decision on the list of types of personal data processing operations for which an assessment of the impact on the personal data protection must be performed and the opinion of the Commissioner for Information of Public Importance and Personal Data Protection must be sought;[33]
(8) Decision on the list of countries, parts of their territories or one or more sectors of certain activities in those countries and international organizations where it is considered that an adequate level of protection of personal data is ensured;[34]
(9) Decision on determining standard contractual clauses,[35] which determines the standard contractual clauses in the contractual relation between a controller and processor; and

27 Official Journal of the Republic of Serbia 35/2009.
28 Official Journal of the Republic of Serbia 50/2009.
29 Official Journal of the Republic of Serbia 40/2019.
30 Ibid.
31 Ibid.
32 Ibid.
33 Official Journal of the Republic of Serbia 45/2019, 112/2020.
34 Official Journal of the Republic of Serbia 55/2019.
35 Official Journal of the Republic of Serbia 5/2020.

(10) Rulebook on the form of identification card of the authorized person for performing inspection supervision in accordance with the LPPD.[36]

The LPPD is an "umbrella regulation" in the field of personal data protection in Serbia. Sectoral laws also apply to personal data processing in particular areas. The LPPD lays down general rules on personal data protection, while other laws may prescribe specific legal regimes applicable in certain areas or for certain type of activities. However, the principle *lex specialis derogate legi generali* does not apply, since the LPPD explicitly requires that the provisions of other laws regulating the processing of personal data must be in line with the LPPD.[37] There are numerous sectoral laws adopted in the last fifteen years in Serbia:

(1) Law on Electronic Communications[38] regulates interception of communications;
(2) Law on Electronic Commerce[39] regulates electronic marketing;
(3) Law on Consumer Protection[40] regulates electronic marketing;
(4) Law on Advertising[41] regulates electronic marketing;
(5) Law on Patients' Rights[42] regulates the duty of health professionals to keep the patients' personally identifiable information confidential;
(6) Labor Law[43] regulates the processing of personal data within the employment sector;
(7) Law on Labor Records[44] regulates the collecting of the personally identifiable data in the employment sector;
(8) Law on Healthcare Documentation and Healthcare Records[45] regulates the collecting of the personally identifiable information in the healthcare sector;
(9) Law on High Education[46] regulates the processing of the personally identifiable information within the sector of higher education;
(10) Law on the Education System[47] regulates the processing of the personally identifiable information within the education sector;

36 Official Journal of the Republic of Serbia 61/2019.
37 Art. 2, para. 2 of LPPD.
38 Official Journal of the Republic of Serbia 44/2010, 60/2013, 62/2014 and 95/2018.
39 Official Journal of the Republic of Serbia 41/2009, 95/2013 and 52/2019.
40 Official Journal of the Republic of Serbia 88/2021.
41 Official Journal of the Republic of Serbia 6/2016 and 52/2019.
42 Official Journal of the Republic of Serbia 45/2013 and 25/2019.
43 Official Journal of the Republic of Serbia 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017, 113/2017 and 95/2018.
44 Official Journal of the FR Yugoslavia 46/96; Official Journal of the Republic of Serbia 101/2005 and 36/2009.
45 Official Journal of the Republic of Serbia 123/2014, 106/2015, 105/2017 and 25/2019.
46 Official Journal of the Republic of Serbia 88/2017, 73/2018, 27/2018, 67/2019, 6/2020, 11/2021, 67/2021 and 67/2021.
47 Official Journal of the Republic of Serbia 88/2017, 27/2018, 10/2019, 27/2018, 6/2020 and 129/2021.

(11) Law on Pension and Disability Insurance[48] regulates the collecting of the personally identifiable information within the sector of pension and disability insurance; and
(12) Law on Health Insurance[49] regulates the collecting of the personally identifiable information within the health insurance sector.

The right to privacy enjoys protection in civil law. Under Art. 157 of the Law on Contracts and Torts (LCT),[50] everyone is entitled to demand that the court or other competent authority order the cessation of an action by which the integrity of an individual and integrity of family life, as well as other rights pertaining to a person, is violated. In case of a violation of privacy, the general principles of civil wrongs (torts) shall apply.[51] More specifically, with respect to the data protection right, the LPPD explicitly provides for an individual's right to receive compensation from the controller or processor for the material or nonmaterial damage suffered.[52]

The right to privacy enjoys protection in criminal law, as well. The Penal Code of the Republic of Serbia (PC)[53] prescribes several criminal offences that are directly or indirectly in relation to the breach of privacy:

(1) violation of privacy of letter and other mail (including emails);[54]
(2) violation of a home;[55]
(3) illegal search of an apartment, premises or person;[56]
(4) unauthorized disclosure of a secret;[57]
(5) unauthorized wiretapping and recording;[58]
(6) unauthorized photographing;[59]
(7) unauthorized publication and presentation of another's texts, portraits and recordings;[60]
(8) unauthorized collection of personal data;[61]

48 Official Journal of the Republic of Serbia 34/2003, 64/2004, 84/2004, 85/2005, 101/2005, 63/2006, 5/2009, 107/2009, 101/2010, 93/2012, 62/2013, 108/2013, 75/2014, 142/2014, 73/2018, 46/2019, 86/2019 and 62/2021.
49 Official Journal of the Republic of Serbia 25/2019.
50 Official Journal of the SFR Yugoslavia 29/78, 39/85, 45/89 and 57/89; Official Journal of the FR Yugoslavia 31/93; Official Journal of Serbia and Montenegro 1/2003; Official Journal of the Republic of Serbia 18/2020.
51 Arts. 154–155, 158–161, 164–169, 185–186, 198–205 of LCT.
52 Art. 84 of LPPD.
53 Official Journal of the Republic of Serbia 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.
54 Art. 142 of PC.
55 Art. 139 of PC.
56 Art. 140 of PC.
57 Art. 141 of PC.
58 Art. 143 of PC.
59 Art. 144 of PC.
60 Art. 145 of PC.
61 Art. 146 of PC.

(9) dissemination of information on personal and family life;[62]
(10) showing, procuring, and possessing pornographic material of minors;[63]
(11) abuse of computer networks or other technical means of communication for committing criminal offences against sexual freedom of the minor;[64]
(12) unauthorized access to computer, computer network or electronic data processing;[65]
(13) unauthorized use of a computer or computer network;[66] and
(14) violation of confidentiality of proceedings.[67]

Further to criminal liability, several laws prescribe penalties for misdemeanors. For example, if the personally identifiable information has not been collected or processed lawfully, the LPPD empowers the Commissioner for Information of Public Importance and Personal Data to impose pecuniary fines for misdemeanors or to initiate misdemeanor proceedings before the competent court.[68] In such a case, the provisions of the Law on misdemeanors[69] must be observed.

The legal framework for the protection of privacy and personal data in the Republic of Serbia includes administrative remedies as well. Under the LPPD, the data subject (natural person whose personal data is processed) has the right to lodge a complaint before the Commissioner for Information of Public Importance and Personal Data, if they believe that the processing of their personal data was performed contrary to the law. Data subject, data processor or any other natural or legal person concerned by the Commissioner's decision may initiate an administrative dispute, within 30 days following the receipt of such decision.[70] Administrative disputes fall under jurisdiction of the Administrative Court and are conducted pursuant to the Law on administrative disputes.[71]

Although the Republic of Serbia is not an EU Member State, the European Union's General Data Protection Regulation may, under specific circumstances, be applicable in the Serbian context. Under Art. 3.2 of the GDPR, the regulation applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether

62 Art. 172 of PC.
63 Art. 185 of PC.
64 Art. 185b of PC.
65 Art. 302 of PC.
66 Art. 304 of PC.
67 Art. 337 of PC.
68 See for example Arts. 79, 95 of LPPD. The Commissioner may impose pecuniary fines for misdemeanors directly in case the latter are prescribed in fixed amounts. However, if the amount of a fine depends on the assessment of circumstances of the breach, i.e., there is a range prescribed by the law, the Commissioner must initiate misdemeanor proceedings before the competent court.
69 Official Journal of the Republic of Serbia 65/2013, 13/2016, 98/2016, 91/2019 and 91/2019.
70 Art. 83 of LPPD.
71 Official Journal of the Republic of Serbia 111/2009.

a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.[72] This means that companies that have a connection with the European market must follow the same standard of data protection practiced by European companies.[73]

## 4. Privacy as a value

Privacy is a concept which is widely regarded as contested. As sociologist Alan Westin said, "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists."[74] Privacy is a relatively modern concept, whose importance increased with the development of digital technologies. Since 1970s, the growing use of mainframe computers by states and large corporations, convened experts and policy-makers to explore the risks and develop protections for privacy. The use of computers and in particular the Internet have "commercialized" areas which were previously the individual domain. The omnipresence of both traditional and social media transformed the way we conduct our everyday activities. The information about our habits, our actions, and our beliefs are systematically being collected by various actors. Furthermore, such information may instantly be made accessible to a worldwide audience. Living in "a state of permanent visibility" highlights the importance of protection of privacy and personal data.[75]

There are different theoretical approaches to the concept of privacy. The "skeptical" approach sees privacy as a parasitic interest which derives its value from other more fundamental entitlements. Under this reductionist view, privacy claims should be more properly characterized as assertions of other interests; in particular, property rights, and rights in respect of the person.[76] The lighter "skeptical" theory does not see the privacy as a concept without value, but rather as an individual's interest in maintaining exclusivity over his or her body or property. Contrary to reductionist theories, intuitionism suggests the existence of a consensus that privacy has value, but it is unable to authoritatively determine what that value practically entails.[77] The intuitionist approach to this concept has led to different definitions of privacy, one of them being "the right to be let alone." This

72 For a more detailed analysis of extraterritorial application of the GDPR, see Greze, 2019, pp. 109–128.
73 Jaeger Junior and Copetti Cravo, 2021, p. 367.
74 Westin, 1967, p. 5.
75 Delany and Carolan, 2008, p. 1.
76 Ibid. p. 4.
77 Ibid. p. 6.

definition has been particularly influential in the constitutional sphere, where it has been frequently invoked in support of individual's claims to freedom from the state's intervention. However, a right to privacy which would apply only against the state does not offer the individual adequate protection. It is too narrow to capture the potential range of privacy infringement, since privacy interests may be undermined by non-public (non-state) actors.[78] Nevertheless, the definition of privacy as "the right to be let alone" need not necessarily be interpreted restrictively. It could be understood as a shield not only against the state actors, but against everyone. Another intuitionist approach to privacy defines it in terms of individual's inaccessibility. The simplistic interpretation of this definition would mean that when an individual is out of reach of all external actors, he or she is said to be enjoying "perfect privacy."[79] Finally, an intuitionist approach to privacy may lead us to understanding it as specific "natural" zones within which privacy interests arise and ought to be protected. These natural areas are usually identified as the home and the body.[80]

The analysis of privacy as a value leads us inevitably to exploring the possible religious roots to this concept. Since Serbia's population is predominantly of Orthodox Christian religion, we focus on the exploration of a possible Christian background of the concept of privacy. Today, the right to privacy is comprehended as a human right. The approach of Orthodox Christian churches[81] to human rights is cautious. This reflects the approach of the Orthodox Church to modernism. Contrary to the Catholic Church, the Orthodox Church entered the modern world from the period of Ottoman rule. The brief period of liberty was soon replaced by the repression of Communist regimes. Consequently, the Orthodox Church found itself astounded by modernism and did not have enough time to react to such social changes. This resulted in a variety of disharmonized approaches to human rights in mid-20th century and later.[82]

One of the notable examples of the Orthodox Church's approach to human rights is that of a social doctrine called "The Principles of Social Conception of the Russian Orthodox Church," adopted at the Bishops Council meeting in Moscow in August 2000. Under this doctrine, human rights cannot be superior to the values of the spiritual world. It is "inadmissible and dangerous," therefore, to interpret human rights as the ultimate and universal foundation of societal life to which religious views and practice should be subjected. From the point of view of the Orthodox Church, the political and legal institution of human rights can promote the good

78 Ibid. p. 7.
79 Ibid. p. 8.
80 Ibid. p. 9.
81 The Orthodox Church is made up of a number of self-governing churches which are either "autocephalous" (having their own head) or "autonomous" (self-governing). The Orthodox Churches are united in faith and by a common approach to theology, tradition, and worship. One of the autocephalous churches is the Serbian Orthodox Church.
82 Božović, 2020, p. 54.

goals of protecting human dignity and contribute to the spiritual and ethical development of the personality. One's human rights cannot be set against the values and interests of one's homeland, community, and family.[83] In June 2008, the Russian Orthodox Church adopted a document called "The Basic Principles of the Russian Church Teaching on Human Dignity, Freedom, and Rights" in which for the first time it takes a clear position on the right to privacy, particularly in the digital context:

> People's private life, worldview, and will should not become a subject of total control. Any manipulation over people's choice and their conscience by power structures, political forces and economic and media elites is dangerous for a society. Such things as compilation, concentration, and use of information about any aspect of people's life without their consent are also inadmissible. Information about a person can be collected without his or her consent only in cases where it is required for the defense of the homeland, preservation of morality, protection of people's health, rights and legitimate interests or the need to investigate a crime and to exercise justice. But in these cases, too, information may be collected and used in conformity with the stated aims and in accordance with law. The methods of collecting and processing information about people should not hurt the dignity of a person, restrict his freedom, or turn him from a subject of public relations into an object of machine operation. The adoption of technical devices accompanying a person permanently or inseparable from his body will be even more dangerous for human freedom if used to control his personality.[84]

More recently, at the Holy and Great Council of the Orthodox Church held in June 2016 in Crete (Greece), in the document entitled "The Mission of the Orthodox Church in Today's World," it has been emphasized that the Orthodox Church considered that every human being, regardless of skin color, religion, race, sex, ethnicity, and language, is created in the image and likeness of God, and enjoys equal rights in society. Consistent with this belief, the Orthodox Church rejects discrimination for any of the aforementioned reasons since these presuppose a difference in dignity between people. Although the quoted document does not refer to the right to privacy, it does show the alleviating of the Orthodox Church's general approach to human rights. This trend may be explained by the readiness of the Church to make use of the concept of human rights to protect its own institutional rights, as well as the individual rights of its believers.[85]

83 Novik, 2002, p. 12.

84 The Russian Orthodox Church's Basic Teaching on Human Dignity, Freedom and Rights, Section IV "Human dignity and freedom in the system of human rights", para. 7. [Online] Available at: https://old.mospat.ru/en/documents/dignity-freedom-rights/iv/ (Accessed: 23 February 2022).

85 Božović, 2020, p. 56.

## 5. Fundamental grounds for protecting the right to privacy

In Serbian law, the notion of privacy was initially employed to designate the protection of personal and family life, the protection of the home, and the protection of correspondence. In modern times, the concept of privacy is understood as the protection of personally identifiable data. The Serbian legal doctrine differentiates between general personal right and specific personal rights. The right to privacy is traditionally classified among specific personal rights, altogether with the right to identity, the right to a good name (derived from the right to human dignity), the right to respect of a deceased person.[86] The evolution of the concept of privacy is reflected in the constitutional history of Serbia. The earliest traces of the protection of privacy may be found in the Constitution of the Kingdom of Serbia, proclaimed on December 22, 1888. Under Art. 15 of the 1888 Constitution, the privacy of home may not be violated, except in cases prescribed by the law. A warrant to search the premises must be issued by a judge. The search must be conducted in presence of at least two witnesses who are Serbian citizens. The search may not be conducted during the night. Under Art. 23 of the 1888 Constitution, the secrecy of letters and telegraph messages may not be violated, except in cases of a criminal investigation or a war. The law is to prescribe which state organs are responsible for the breach of privacy of correspondence. The subsequent constitutions have also protected certain aspects of privacy. For example, the Constitution of the Socialist Federal Republic of Yugoslavia, proclaimed on February 21, 1974, guaranteed the inviolability of integrity of a person, personal and family life, and other rights of a person.[87] The 1974 Constitution proclaimed the inviolability of the home, which may be violated only in cases prescribed by the law.[88] The inviolability of letters and other means of communication was also guaranteed, except in case of a criminal investigation or if that is justified by the reasons of national security.[89] In contrast with the previous "particularized" approach, the Constitution of the Federal Republic of Yugoslavia, proclaimed on 27 April 1992, guaranteed the inviolability of all personal rights, without indicating any exception beforehand: "The inviolability of the physical and psychological integrity of the individual, his privacy and personal rights shall be guaranteed. The personal dignity and security of individuals shall be guaranteed."[90]

The current Constitution of the Republic of Serbia,[91] proclaimed on November 8, 2006, does not lay down a general right to privacy. Instead, it prescribes several

86 Vodinelić, 2014, pp. 258–271.
87 Art. 176 of the Constitution of the Socialist Federal Republic of Yugoslavia, Official Journal of the SFR Yugoslavia 9/1974.
88 Ibid. Art. 184.
89 Ibid. Art. 185.
90 Constitution of the Federal Republic of Yugoslavia, Official Journal of the FR Yugoslavia 1/1992, Art. 22.
91 Constitution of the Republic of Serbia, Official Journal of the Republic of Serbia 98/2006.

specific rights and liberties which, directly or indirectly, protect the private sphere of individuals. In that sense, the Constitution protects dignity and free development of individuals, and guarantees the inviolability of physical and mental integrity of individuals, the inviolability of the home, the confidentiality of letters, and other means of communication, as well as the freedom of thought, conscience, and religion. Additionally, the Constitution lays down a separate right to personal data protection. Currently, there are no plans for the constitutional amendments that would comprise any of these privacy-related provisions.[92]

Under Art. 23 of the Constitution, human dignity is inviolable, and everyone is obliged to respect and protect it. A violation of privacy would typically violate human dignity as well, i.e., the illegal posting of one's private explicit photos online or the publication in the media of one's medical records. A breach of privacy may also violate one's mental integrity, which is guaranteed, together with physical integrity, under Art. 25 of the Constitution. The highest national legal act guarantees the inviolability of the home. Under Art. 40 of the Constitution, no one may enter one's home or other premises against the will of its tenant, nor conduct a search in them. The tenant of the home or other premises has the right to be present during the search, in person or through his legal representative, together with two other witnesses who must not be minors. Entering one's home or other premises, and in special cases conducting a search without witnesses, is allowed without a court order if necessary for the purpose of the immediate arrest and detention of a perpetrator of a criminal offence, or to eliminate the direct and grave danger for citizens or property under conditions prescribed by the law. The Constitution also guarantees the confidentiality of letters and other means of communication. This provision may be interpreted as to include emails as "other means of communication." Under Art. 41 of the Constitution, derogation from this prohibition is allowed only for a specified period and based on decision of the court if this is necessary to conduct criminal proceedings or to protect the safety of the Republic of Serbia, in a manner stipulated by the law. The right to privacy is also protected through the constitutional guarantee of the freedom of thought, conscience, and religion laid down under Art. 43, in the sense that the citizens do not have the obligation to declare their religious or other beliefs. Finally, Art. 42 of the Constitution prescribes a separate right to personal data protection. Collecting, keeping, processing, and using of personal data is further regulated by the law. The use of personal data for purposes other than those for which they were collected is prohibited and punishable by law, unless this is necessary to conduct criminal proceedings or protect safety of the Republic of Serbia, in a manner stipulated by law. The Constitution also lays down the right to be informed about the personal data that is being collected, in accordance with the law, and the right to court protection in case of the abuse of such data. By prescribing a separate right to personal data protection,

92 On January 16, 2022, at a constitutional referendum, the Serbian citizens approved the constitutional amendments which would introduce the changes in the election of judges and prosecutors.

the Serbian constitution-makers were influenced by the Charter of Fundamental Rights of the European Union, which distinguishes data protection from privacy in the traditional sense, and lays down some specific guarantees of personal data protection.[93]

Human and minority rights that are guaranteed by the Constitution are implemented directly. The Constitution guarantees and directly implements human and minority rights guaranteed by the generally accepted rules of international law, ratified international treaties, and laws. The law may prescribe manner of exercising these rights only if explicitly stipulated in the Constitution or necessary to exercise a specific right owing to its nature, whereby the law may not under any circumstances influence the substance of the relevant guaranteed right. Provisions on human and minority rights are interpreted to the benefit of promoting values of a democratic society, pursuant to valid international standards in human and minority rights, as well as the practice of international institutions which supervise their implementation.[94] Human and minority rights guaranteed by the Constitution may be restricted by the law if the Constitution permits such restriction and for the purposes allowed by the Constitution, to the extent necessary to meet the constitutional purpose of restriction in a democratic society and without encroaching upon the substance of the relevant guaranteed right. The level of human and minority rights attained may not be lowered. When restricting human and minority rights, all state bodies, particularly the courts, are obliged to consider the substance of the restricted right, pertinence of restriction, nature and extent of restriction, relation of restriction and its purpose, and possibility to achieve the purpose of the restriction with less restrictive means.[95]

The Constitution lays down the right to judicial protection in case human or minority rights guaranteed by the Constitution have been violated or denied. The citizens also have the right to elimination of consequences arising from the violation. Under Art. 170 of the Constitution, a constitutional appeal may be lodged against individual acts or actions of state bodies or organizations entrusted with public powers, which have violated or withheld human and minority rights and freedoms guaranteed by the Constitution. A constitutional appeal may be lodged provided that other legal remedies for the protection of human and minority rights have been exhausted or have not been envisaged. In addition, constitutional appeal may be filed if legal remedies have not been exhausted, as when the submitter of a constitutional appeal has suffered a violation of the right to a trial within a reasonable time. A constitutional appeal may be filed by any (legal or natural) person who holds that their constitutionally guaranteed human or minority right or freedom have been violated by an individual act or action of a state body or organization entrusted with public powers. Hence, a legal or natural person may file a constitutional appeal

93 See Section 1 of this paper.
94 Ibid. Art. 18.
95 Ibid. Art. 20.

only if a violation of their own right is in question, i.e., they must have a personal and real interest that the disputed act is removed. A decision of the Constitutional Court upholding a constitutional appeal is the legal grounds for filing a claim for compensation of damage or removal of other detrimental consequences before a competent body, in accordance with law. According to the Constitutional Court's database, so far, no proceedings related to the breach of privacy in the digital context were initiated.[96]

Citizens also have the right to address international institutions to protect their freedoms and rights as guaranteed by the Constitution.[97] More specifically, with respect to the alleged violation of the right to privacy, Serbian citizens may address the European Court of Human Rights and the United Nations' Human Rights Committee. The ECtHR hears applications alleging that a contracting state has breached one or more of the human rights provisions concerning civil and political rights set out in the European Convention on Human Rights and its protocols. An application can be lodged by an individual, a group of individuals or one or more of the other contracting states. Presently,[98] there is only one case before the ECtHR against the Republic of Serbia with respect to the alleged violation of the right to privacy in the digital environment. The application *Aleksić v. Serbia* concerns the interception and reading of the applicant's emails by his public employer, the Serbian Statistics Office. These emails were sent from the applicant's official account and contained information regarding his personal and his professional circumstances, including comments as to the situation in the office. The emails were subsequently also used as evidence in a civil defamation suit brought against the applicant by one of his colleagues.[99] The ECtHR addressed several questions to the parties, related *inter alia* to the possible interference with the applicant's right to respect for his private and family life or his correspondence, within the meaning of Art. 8, para. 1 of the ECHR, and the compliance of such potential interference with the conditions laid down under Art. 8, para. 2 of the ECHR. The case is pending. The Serbian citizens have also the possibility to address the United Nations' Human Rights Committee, which may consider individual communications alleging violations of the rights set forth in the International Covenant on Civil and Political Rights by States parties to the First Optional Protocol to the International Covenant on Civil and Political Rights. Presently,[100] there are no cases brought against the Republic of Serbia before the United Nations' Human Rights Committee on the grounds of the breach of the right to privacy in the digital context.

96 Situation in February 2022.
97 Ibid. Art. 22.
98 Situation in February 2022.
99 ECtHR, *Aleksić v. Serbia,* application no. 40825/15, 31 July 2015.
100 Situation in February 2022.

## 6. Protection of the right to privacy in civil law

In civil law, the right to privacy enjoys protection under the general principles of civil wrongs (torts). A violation of personality rights would, in principle, generate the duty to compensate of nonmaterial, and more rarely, material damage.[101] Under the general principles of civil wrongs, whoever causes injury or loss to another is liable to redress it, unless proven that the damage was caused without his fault.[102] Injury or loss comprises a diminution of someone's property (simple loss) and preventing its increase (profit lost), as well as inflicting on another physical or psychological pain or causing fear (nonmaterial damage, or mental anguish). Fault exists after a tort-feasor has caused injury or loss intentionally or out of negligence.[103] With respect to the liability of minors, the LCT prescribes that a minor from seven to fourteen years of age is not liable for loss, unless it is proved that he was mentally competent while causing the damage, while a minor older than fourteen shall be liable according to general rules of tort liability.[104] Parents are liable for loss or injury caused by their child of over seven years of age, unless proving that the loss or injury took place without their fault.[105]

In case of violation of an individual right, the court may order that, at the expense of the tort-feasor, the sentence, namely the correction, be made public, or it may order that the tort-feasor takes back the statement causing the violation, or may order something else that would serve the purpose, otherwise it would apt to be achieved by indemnity.[106] For offended reputation, honor, freedom, or rights of personality, as well as for fear suffered, the court may—after finding that the circumstances of the case and particularly the intensity of pains and fear, and their duration, provide a corresponding ground thereof—award equitable damages, independently of redressing the property damage, even if the latter is not awarded.[107] In deciding on the request for redressing nonmaterial loss, as well as on the amount of such damages, the court shall consider the significance of the value violated, and the purpose to be achieved by such redress, but also that it does not favor ends otherwise incompatible with its nature and social purpose. Under the general principles of civil wrongs, at the request by a person sustaining loss the court may also award damages for future general loss if, according to regular course of events, it became certain that it will continue.[108]

These general rules serve to redress the damage suffered from the violation of personality rights, which presupposes that a violation have already occurred.

101 Pajtić, Radovanović, and Dudaš, 2018, p. 520.
102 Art. 154 of LCT.
103 Art. 158 of LCT.
104 Art. 160 of LCT.
105 Art. 165 of LCT.
106 Art. 199 of LCT.
107 Art. 200, para. 1 of LCT.
108 Art. 203 of LCT.

However, these rules do not provide for a mechanism which would protect an injured party from ongoing violations, from repetitive violations or from threats to violate personality rights.[109] This gap is filled by a specific demand to cease with the violation of individual rights. Under Art. 157 of the LCT, everyone is entitled to demand that the court or other competent authority order the cessation of an action by which the integrity of an individual, the integrity of family life, as well as other rights pertaining to a person, is violated. The court or other competent authority may order cessation of the action under the threat of a fine[110] set as a lump sum or a sum per instalments, to the benefit of the person suffering damage. The legislature did not indicate in relation to which personality rights (individual rights) this specific request may be invoked. The dominant view in legal doctrine is that Art. 157 of the LCT may be invoked to protect: (1) the right to human integrity, both physical and mental integrity; (2) the right to inviolability of personal and family life, including the right to privacy of correspondence, the right to protection of a business secret, the protection from illegal audio and video recording, and the inviolability of home; (3) other personality rights, such as the right to health, the right to a good name, the right to freedom, and the right to a personal name.[111] In the online environment, the first situation in which this specific demand to cease with the violation of individual rights may be invoked concerns the case of an ongoing violation consisting, for example, of the permanent availability of a website containing a personally identifiable data or a data that threatens a person's reputation. The second situation in which this demand may be invoked concerns the case where a violation has already taken place (e.g., by publishing untrue information in an online media outlet), and it is probable that a violation will be repeated (e.g., the perpetrator threatens that it will publish the same information in another online media outlet). The final and third scenario concerns the case where a violation have not yet taken place, but it is likely that it will (e.g., a person threatens that it will publish another's personal data online).[112]

More specifically, with respect to the personal data protection right, the LPPD explicitly provides for an individual's right to receive compensation from the controller or processor of personal data for the material or nonmaterial damage suffered.[113] The compensation cannot be obtained in the proceedings before the Commissioner for Information of Public Importance and Personal Data Protection, but in a separate civil law proceedings under the general principles of civil wrongs (torts). If a personal data has been controlled and/or processed by several controllers/

109 Pajtić, Radovanović and Dudaš, 2018, p. 520.

110 The use of the term "fine" requires further clarification. The above-described mechanism is modeled upon the French enforcement mechanism called "astreinte." "Astreinte" is a compensation payment for the delay in the execution of a court decision. Such payment, in contrast to court fines, is paid not to the state, but to the person in whose favor the decision was issued.

111 Perović, 1983, p. 556.

112 Pajtić, Radovanović and Dudaš, 2018, p. 521.

113 Art. 86, para. 1 of LPPD.

processors, they shall bear unlimited solidary/joint responsibility.[114] Also, an individual has the right to initiate civil law proceedings or other court proceedings in case of a violation of one of the rights guaranteed under the LPPD, such as the right to data portability, the right to erasure, the right to restrict personal data processing.[115] Such lawsuit does not preclude the right of an individual to initiate other administrative or court proceedings aiming at protecting his/her rights under the LPPD.[116] The lawsuit is to be lodged before the higher court that has jurisdiction over the territory of residence, domicile, or seat of a personal data controller or its representative, or before the higher court that has jurisdiction over the territory where a person to which data relate has residence or domicile, except if a personal data controller or processor is a state organ.[117]

Further to the general principles of civil wrongs (torts) laid down by the LCT, the Law on Media Services (LMS)[118] may be relied on to protect the personality rights which were injured by a registered media outlet. The Serbian Business Registers Agency runs the Media Register, which represents an integrated electronic database of dailies and periodicals, news agency services, radio programs, television programs, and independent online media editions (editor-formatted online portals).[119] The LMS prohibits the publication of the following information without consent of a concerned person: (1) information pertaining to private life or a personal records (e.g., letter, diary, digital recording); (2) visual recordings (e.g., photograph, drawing, video recording); and (3) audio recordings. Exceptionally, such information may be published without consent of a concerned person, if the audience cannot infer from the published information the identity of a concerned person.[120] A consent given for one specific type of media coverage cannot be interpreted as a consent for a subsequent publication of information within the same or other type of media coverage.[121] If a personal information pertains to a deceased person, a consent to publish may be given by a widow/widower, children who are sixteen years old, parents, brother or sister.[122] A person to which a published information pertains to enjoys the right of reply and the right of correction. If a media outlet rejects to publish a reply or correction, without such action being justified by one of the limitations to the right to privacy, prescribed by the LMS, a concerned person may request from the court to

114 Art. 86, para. 5 of LPPD.
115 Art. 84, para. 2 of LPPD.
116 Art. 84, para. 1 of LPPD.
117 Art. 84, para. 4 of LPPD.
118 Official Journal of the Republic of Serbia 83/2014, 58/2015 and 12/2016.
119 The LMS provides examples of what the media is not (e.g., book, movie, audio and audio-visual support, scientific and professional journals, web browsers, social networks, blogs). Exceptionally, online presentations may be treated as a media outlet within the meaning of the LMS if they are registered as such. See Art. 30.
120 Art. 80 of LMS.
121 Art. 80 of LMS.
122 Art. 84 of LMS. A consent of one of the indicated persons is sufficient even in case another relative objects to the publication of information.

order the reply or correction to be published.[123] A person whose right to privacy is violated by a media outlet may request from the court to: (1) determine that a right to privacy has been infringed; (2) order a media outlet to cease the infringing activity; (3) hand over or destroy the infringing content (e.g., delete an audio or video recordings, or hand over a negative).[124] A person whose right to privacy is allegedly violated may apply for interim measures, aiming at prohibiting the publication of information as long as the court proceedings are pending.[125]

The LMS allows for limitations to the right to privacy, which are justified by reasons of the public interest. The LMS enlists *exempli causa* circumstances under which a media outlet may publish an information pertaining to one's private life, without consent of a concerned party: (1) if information or record was intended to be made public by a concerned person, or if information or record was submitted to the media by a concerned party; (2) if information or record pertains to a person or event of public interest, in particular if it pertains to a public or political figure, and publishing such information is in interest of national security or economic well-being of a country, prevention of crime or disorder, protection of health or public morality, or protection of third party's rights and freedoms; (3) if a concerned party attracted public interest by way of his/her conduct in private, family, or professional life or by his/her public statements, thus creating incentive for media coverage; (4) if information is communicated during parliament session; (5) if publication of such information is in the interest of judiciary or national security; (6) if a concerned person did not object to obtaining the information or to making a recording, although he/she knew that such information/recording will be published; (7) if publication of such information is in the interest of science or education; (8) if publication of such information is necessary to alert the public of a danger (e.g., finding a missing person, or preventing a fraud); (9) if a recording pertains to a number of persons (e.g., concert audience or protesters at rallies); (10) if a recording is made at a public event; (11) if a person's face is made available to public as part of wider recording of an urban or natural site.[126]

The Serbian case law on privacy protection mainly comprises the disputes arising out of media coverage of certain events. Lawsuits often aim at protecting both the right to privacy and the right to reputation and honor. Nevertheless, the Serbian courts are undoubtedly of the view that the right to privacy may also enjoy protection separately and independently from the protection of the right to reputation and honor. This also stems from Art. 8 of the ECHR which directly protects the right to privacy.[127] Court competence in privacy disputes that concern the Internet is shared between the high and basic courts. Under Art. 4, para. 2 of the Law on

123 Arts. 83, 84 of LMS.
124 Art. 101 of LMS.
125 Art. 104 of LMS.
126 Art. 82 of LMS.
127 See for example: Appellate Court in Belgrade, decision no. Gž3 29/19, 1 March 2019; High Court in Belgrade, decision no. P3 br. 439/16, July 3, 2018.

Seats and Territories of the Courts and Public Prosecutors Offices,[128] a high court adjudicates in the first instance, in civil disputes about the printing of corrected information, and responses to information about violations of the prohibition of hate speech, protection of the right to privacy, and failure to publish information and compensation of damages in connection with the publication of the information.[129] However, a basic court shall adjudicate in the first instance if a violation of personality rights which generates the duty to compensate of nonmaterial damage occurred on social networks or other information exchange platforms that are not registered as a media outlet. The latter stems from Art. 22, para. 2 of the Law on Organization of Courts (LOC),[130] which prescribes that a basic court adjudicates in civil disputes in the first instance, unless the disputes are assigned to another court, and conducts enforcement and non-contentious proceedings that are not under the jurisdiction of another court. This interpretation of the rules on court jurisdiction, based on the distinction between registered media outlets and other information exchange platforms, is also reflected in Serbian case law.[131]

There is a significant number of disputes for the violation of privacy between individuals, on the one hand, and web portals and official webpages of Serbian newspapers, on the other, that follow the same pattern: a media outlet first publishes detailed information about the identity and private life of the claimant, which then wins the court case if it proves that he/she cannot be taken as a political or public figure whose private life enjoys lesser privacy protection. For example, a website of a Serbian daily newspaper published an Art. containing details from police records pertaining to a son of a famous chess player who committed a crime. The article contained information about his family ties with a famous chess player (whose name was also published), information about his current and previous employer, and details about the criminal act itself. The Supreme Court of Cassation confirmed the decision of a lower court finding a violation of privacy, showing that a relative of a celebrity is not a public figure within the meaning of the LMS. Consequently, he/she enjoys full privacy protection under Serbian law.[132] Similarly, a Serbian weekly magazine and its website were found to have violated privacy of a famous singer by publishing photographs of her cell phone screen, clearly showing the contents of SMS messages she was exchanging with a friend. Although the claimant was a public figure who enjoys limited privacy protection, the court found that publishing the contents of her SMS exchange without her consent did constitute a violation of

128 Official Journal of the Republic of Serbia 101/13.

129 Judicial power in the Republic of Serbia is vested in courts of general and special jurisdiction. The courts of general jurisdiction are basic courts, higher courts, appellate courts, and the Supreme Court of Cassation.

130 Official Journal of the Republic of Serbia 116/08, 104/09, 101/09, 31/11, 78/11, 101/11 and 101/13.

131 See for example: Appellate Court in Belgrade, decision no. R 210/17, 15 August 2017; Third Basic Court in Belgrade, decision no. 16P 1761/17, April 25, 2017; Supreme Court of Cassation, decision no. R1. 161/19, 20 March 2019; Supreme Court of Cassation, decision no. P1 263/2021, April 29, 2021.

132 Supreme Court of Cassation, decision no. Rev 405/2015, February 18, 2016.

the right to privacy. The court ordered that the magazine or its editor-in-chief compensate for the nonmaterial damage.[133] Conversely, if a website observes its duties under the LMS and the journalistic code of ethics, it shall not be responsible for a violation of privacy of a public or political figure. For example, a webpage of a Serbian daily newspaper published an article about a political figure in which it stated that she is under investigation for abuse of state funds. The article also stated that the claimant's domestic partner was allegedly involved in a similar criminal act. Prior to publishing the article, the journalist contacted the claimant, who confirmed the identity of her partner and the fact that there is an ongoing criminal investigation. The court found that the respondent merely published information that was either already in public domain or confirmed by the claimant, in full observance of the provisions of the LMS. Therefore, the court found no breach of privacy in the case.[134] Finally, if a web-portal simply reposts an article taken from another news outlet, while clearly indicating the source of information, it shall not be liable for privacy and/or reputation infringement, even if the information is inaccurate or offensive. This view has been taken by the Supreme Court of Cassation, which found no violation of provisions of the LMS in case of re-publishing of an online article containing both a false information that the claimant abused public funds and an offensive information that the claimant belongs to a political party with extremist views.[135]

The civil law proceedings for privacy breaches that do not involve online media outlets (as respondents) are less frequent. Citizens tend to initiate administrative proceedings before the Commissioner for Information of Public Importance and Personal Data Protection more often than civil law court proceedings, even though the compensation for material or nonmaterial damage suffered can only be obtained in the civil court. One of the rare examples to the contrary involves an employee whose personal data regarding an ongoing labor dispute with her employer, as well as data regarding her health status, were made available to her colleagues via the employer's web app. The injured party first notified the Commissioner for Information of Public Importance and Personal Data Protection of the privacy breach, which carried out an inspection and issued a warning to the employer–owner of the web app. The employee then initiated civil law proceedings before the First Basic Court in Belgrade for violation of personality rights and violation of reputation and honor, requesting nonmaterial damage compensation.[136] The first instance court found that the claimant did not prove it suffered any damage because of the defendant's conduct. However, the appellate court in Belgrade overturned the first instance court's decision, finding that non-pecuniary damage to personality rights (but not to honor and reputation) was proven by simply referring to the Commissioner's prior inspection and its findings.[137]

133 Supreme Court of Cassation, decision no. Rev 1903/2016, March 1, 2017.
134 Supreme Court of Cassation, decision no. Rev. 2347/2017, June 6, 2018.
135 Supreme Court of Cassation, decision no. Rev. 2163/2017, January 24, 2018.
136 First Basic Court in Belgrade, decision no. anonymized, March 17, 2021.
137 Appellate Court in Belgrade, decision no. anonymized, August 24, 2021.

## 7. Protection of the right to privacy in criminal law

The Penal Code of the Republic of Serbia (PC) prescribes criminal liability for breaches of privacy, which form subject-matter of several offences, belonging to different categories of criminal offences: (1) criminal offences against rights and freedoms of citizens; (2) criminal offences against honor and reputation; (3) sexual offences; (4) criminal offences against the security of computer data; and (5) criminal offences against the judiciary.

Within the category of criminal offences against rights and freedoms of citizens, the following criminal offences regard direct or indirect breaches of privacy: (1) violation of privacy of correspondence and other mail; (2) violation of the home; (3) illegal search of an apartment, premises, or person; (4) unauthorized disclosure of a secret; (5) unauthorized wiretapping and recording; (6) unauthorized photographing; (7) unauthorized publication and presentation of another's texts, image, or recordings; and (8) unauthorized collection of personal data. Under Art. 142 of the PC, anyone who violates the privacy of electronic mail may be punished with fine or imprisonment up to two years. The penalty may also be imposed to whoever communicates to another the content of another's mail, telegram or consignment acquired by violating the privacy thereof, or makes use of such contents. If the offence is committed by an official in discharge of duty, such a person may be punished with imprisonment from six months to three years. Under Art. 139 of the PC, an infringement of the inviolability of the home is sanctioned. However, such violation is unrelated to the Internet. Similarly, Art. 140 of the PC (illegal search of an apartment, premises, or person) protect one's privacy, but not in an online context. Under Art. 141 of the PC, a lawyer, physician, or other person who discloses without permission a secret that has come to his or her knowledge during the performance of his or her professional duty, shall be punished with fine or imprisonment up to one year. Such a disclosure of a secret may take place both offline and online. Under Art. 143 of the PC, anyone who wiretaps or records conversations, statements, or announcements that is not intended for him or her, using special equipment to do so, shall be punished with fine or imprisonment from three months to three years. Extensively interpreted, this would also allow sanctioning any person who records such statements made online, e.g., within an intercepted video call. The penalty may also be imposed on anyone who enables a third party to be informed about the conversation, statement, or announcement obtained through unauthorized wiretapping or audio recording. Under Art. 144 of the PC, whoever without authorization makes a photograph, film, video, or other recording of another, thereby significantly violating his/her personal life, or who delivers such a recording to a third party or otherwise enables him/her to familiarize himself/herself with the contents thereof, shall be punished with a fine or imprisonment of up to one year. If the offence is committed by an official in discharge of his/her duty, such person shall be punished with imprisonment up to three years. Under Art. 145 of the PC, whoever publishes or publicly presents another's text, portrait, photograph, film, or audio recording

of a personal character without the consent of a person who has drawn up the text or to whom it is related, or without consent of the person depicted in the portrait, photograph or film or whose voice is recorded on audio, or without consent of the person whose consent is mandatory by law, and thereby significantly violates the private life of that person, shall be punished with a fine or imprisonment up to two years. If the offence is committed by an official in discharge of duty, the offender shall be published by imprisonment up to three years. For example, the Basic Court in the municipality of Prokuplje sentenced the editor-in-chief of an online portal who published a photograph of a woman that was taken and published without her consent. The photograph was used to illustrate an article, the contents of which were completely unrelated to the photographed woman. The Basic Court found that the online portal breached the privacy of the photographed woman, and sentenced its editor-in-chief to three months' home detention, without imposing an electronic monitoring measure. The Supreme Court of Cassation upheld the decision.[138]

The introduction of data protection rules into the Serbian legal system led to the amendments of the PC that resulted in prescribing a specific criminal offence sanctioning the unauthorized collection of personal data. Under Art. 146 of the PC, anyone who, without proper authorization, obtains, communicates to another, or otherwise uses information that is collected, processed, and used in accordance with law, for purposes other than those for which they are intended, shall be punished with a fine or imprisonment up to one year. The penalty may also be imposed on anyone who, contrary to law, collects personal data on citizens and uses the data so collected. If the offence is committed by an official in discharge of duty, he/she will be punished with imprisonment up to three years. To interpret the precited provisions one primarily needs to refer to the LPPD, which lays down the definition of data processing, as well as the principles which must be upheld during data processing. Under Art. 4 of the LPPD, data processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The LPDP prescribes certain principles which must be upheld during data processing. The processing must be lawful, fair, and transparent; it must be limited in proportion to the goal and limited only to the data truly necessary; the data must be protected and kept not longer than is necessary to achieve the aim of the processing.[139] All forms of the criminal offence are adjudicated by a basic court in summary proceedings.[140] Committing some of the forms of this criminal offence can contain elements of another criminal offence, such as the unauthorized wiretapping or recording. In such a

138 Supreme Court of Cassation, decision no. Kzz 1383/2019, January 23, 2020.

139 Art. 5 of LPPD.

140 Art. 22 para 1 of LOC; Criminal Procedure Code, Official Journal of the Republic of Serbia 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 and 62/2021, Art. 495.

case, these criminal acts can converge with the unauthorized collection of personal data.[141] The available statistics from 2018 shows that only two persons were accused for the criminal offence of unauthorized collection of personal data, out of total of 1394 persons accused for all criminal offences against rights and freedoms of citizens, which represents 0.14% of all accused persons for that category of offences.[142]

Within the category of criminal offences against honor and reputation, one criminal offence regard direct or indirect breaches of privacy, i.e., dissemination of information on personal and family life. Under Art. 172 of the PC, whoever disseminates information about anyone's personal or family life that may harm his/her honor or reputation, shall be punished with a fine or imprisonment up to six months. If the offence is committed through press, radio, television, or other media or at a public gathering, the offender shall be punished with a fine or imprisonment up to one year. If such dissemination of personal information resulted or could have resulted in serious consequences for the injured party, the offender shall be punished with imprisonment for up to three years. The harm to one's honor or reputation must be proved, and the former must be explicitly stated in the court decision.[143] The offender shall not be punished for disseminating information on personal or family life in discharge of official duty, journalist profession, defending a right or defending justifiable public interest, if he/she proves the veracity of his/her allegations or if he/she proves reasonable grounds for belief that the allegations he/she disseminated were true. The criminal offence of dissemination of information on personal and family life may be conducted against a deceased person as well. In such a case, the incrimination protects the honor and reputation of deceased person's relatives.[144]

Within the category of sexual offences, the following criminal offences regard direct or indirect breaches of privacy: (1) showing, procuring, and possessing pornographic material and underage pornography; and (2) abuse of computer networks or other technical means of communication for committing criminal offences against sexual freedom of the minor. Under Art. 185 of the PC, whoever uses a minor to produce photographs, audio-visual or other items of pornographic content or for a pornographic show, shall be punished with imprisonment of six months to five years. If the act is committed against a child, the offender shall be punished with imprisonment of one to eight years. Also, whoever procures for himself or another and possesses, sells, shows, publicly exhibits, or electronically or otherwise makes available pictures, audio-visual or other items of pornographic content resulting from abuse of minor person, shall be punished with imprisonment of three months to three years. Whoever uses the means of information technologies to deliberately access the photographs, audio-visual or other items of pornographic content resulting from the abuse of a minor shall be punished with a fine or imprisonment of up to six months. Under

141 Sekulić and Grujić, 2020, p. 372.
142 Ibid. p. 374.
143 Supreme Court of Cassation, decision no. Kzz 1030/20, 7 October 2020.
144 Delić, 2022, p. 91.

Art. 185b of the PC, whoever with intent to commit sexual offence, by using computer network or communication with other technical devices makes appointment with a minor and appears on the place of the appointment, shall be punished with imprisonment of six months to five years (eight years in case of a child) and with fine.

Within the category of criminal offences against security of computer data, the following criminal offences regard direct or indirect breaches of privacy: (1) unauthorized access to computer, computer network or electronic data processing; (2) unauthorized use of a computer or computer network. Under Art. 302 of the PC, whoever, by circumventing protection measures, accesses a computer or computer network without authorization, or accesses electronic data processing without authorization, shall be punished by fine or imprisonment up to six months. Whoever records or uses data obtained in such a way, shall be punished by fine or imprisonment up to two years. Under Art. 304 of the PC, whoever uses computer services or computer network with intent to acquire unlawful material gain for himself or another, shall be punished by fine or imprisonment up to three months.

Finally, within the category of criminal offences against the judiciary, one of them regards breaches of privacy: a violation of confidentiality of proceedings. Under Art. 337 of the PC, whoever without authorization discloses what he has learned in court, misdemeanor, administrative, or other procedure established under law, when the law stipulates that such information may not be publicized or if declared secret by a decision of the court or other competent body, shall be punished by fine or imprisonment up to one year. Whoever without permission of the court publishes the course of proceedings against a juvenile or the disposition reached in such proceedings or who publishes the name of the juvenile against whom proceedings were conducted or information that may reveal the identity of the juvenile shall be punished with imprisonment up to two years. Whoever without authorization discloses information on the identity or personal data of a person protected in criminal proceedings or data regarding special protection program, shall be punished by imprisonment of six months to five years.

## 8. Personal data protection in administrative law

The main piece of legislation currently regulating personal data protection in the Republic of Serbia is the Law on Protection of Personal Data (hereinafter, the LPPD),[145] adopted in November 2018 and applicable since August 2019. The LPPD defines a personal data as any information relating to a natural person whose identity is determined or identifiable, directly or indirectly, in particular by reference to an identifier such as a name and identification number, location data, an online

145 For complete references, see Section 3 of this chapter.

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[146] The LPPD applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Furthermore, the LPPD applies to the processing of personal data performed by a controller or a processor that has its business seat/place of residence in the territory of the Republic of Serbia, within the framework of activities performed in the territory of the Republic of Serbia, regardless of whether the processing takes place in the territory of the Republic of Serbia or not. The LPPD also applies to the processing of personal data of data subjects residing in the territory of the Republic of Serbia by a controller or processor who does not have its business seat/place of residence in the territory of the Republic of Serbia, where the processing activities are related to: (1) the offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the territory of the Republic of Serbia; and (2) the monitoring of data subject's behavior as far as their behavior takes place within the territory of the Republic of Serbia. The LPPD does not apply to the processing of personal data by a natural person during a purely personal or household activity.[147] By reason of the matter, the LPPD covers all forms of use or other processing of personal data. The LPPD defines personal data processing as any action taken in connection with the information, including collection, recording, transcription, multiplication, copying, transmission, search, classification, storage, separation, adaptation, modification, making available, use, dissemination, recording, storage, disclosure through transmission or otherwise, dislocation, or other actions carried out in connection with the personal data, regardless of whether such actions are automated, semi-automated, or otherwise carried out.

Following the EU's GDPR model, the LPPD prescribes several specific rights of a data subject. First, the data subject has the right to be informed. The controller is obliged to respond appropriately to provide to the data subjects and prescribed information, i.e., information concerning the exercise of rights, in concise, transparent, intelligible, and easily accessible from, using clear and plain language if the information is intended for a minor. Second, the data subject has the right to request from the controller access to personal data. Third, the data subject has the right to have their inaccurate personal data rectified without undue delay. Fourth, the data subject has the right to have their personal data deleted by the controller when: (1) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed; (2) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing; (3) the data subject objects to the processing and there are no overriding legitimate grounds for the processing; (4) the personal data have been unlawfully processed; (5)

146 Art. 4 of LPPD.
147 Ibid. Arts. 1–3.

the personal data has to be erased for compliance with a legal obligation; or (6) the personal data has been collected in relation to the offer of information society services.[148] Fifth, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling. Sixth, the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, if: (1) the processing is based on consent or a contract; and (2) the processing is carried out by automated means. Seventh, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, if such decision produces legal effects concerning to the data subject or in a similar manner significantly affects the data subject. However, the data subject may consent to such automated processing, or the latter may be explicitly allowed by the law in specific cases. Eight, the data subject has the right to lodge a complaint before the Commissioner, if they believe that the processing of their personal data was performed contrary to the LPPD. Lodging a complaint before the Commissioner does not affect the data subject's right to initiate other administrative or judicial proceedings.[149]

The LPPD prescribes additional rules with respect to the processing of specific categories of personal data: the LPPD prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[150] Exceptionally, the said prohibition does not apply in certain cases prescribed by the LPPD, such as when: (1) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except when it is prescribed that the consent is not a legal basis for such processing; (2) processing is necessary to protect the vital interests of the data subject or of another natural person if the data subject is physically or legally incapable of giving consent; (3) processing relates to personal data that are manifestly made public by the data subject; (4) processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity; (5) processing is necessary for reasons of substantial public interest envisaged by law, if such processing is proportionate to the aim pursued, respecting the essence of the right to data protection and provided that the implementation of suitable and specific measures to safeguard the fundamental rights and the interests of the data subject is ensured.

148 See Midorović, 2019, pp. 293–296.

149 However, a possibility that a number of state authorities at the same time discuss one and the same legal matter may lead to opposite decisions being passed by these authorities.

150 Art. 17 of LPPD.

The national data protection authority responsible for overseeing the implementation of the LPPD is the Commissioner. The latter has the right to access and examine personal data, all documents relating to collection of personal data, personal data controllers' general enactments, and premises and equipment that the controllers use. The Commissioner supervises personal data controllers by conducting inspections. The inspectors act upon information acquired *ex officio* or received from complainants. According to the most recent report, the Commissioner completed 303 inspections in 2021,[151] and received total of 211 complaints for alleged breaches of data protection rules in the same period.[152] If in the process of supervision, the Commissioner establishes a breach of the LPPD, it may issue of warnings or orders. The Commissioner may: (1) order the rectification of the irregularity within a specified period; (2) temporarily ban the processing carried out in breach of the provisions of the LPPD; or (3) order deletion of the personal data collected without a proper legal basis. Certain breaches of law are set out as misdemeanors for which the LPPD prescribes fines. The Commissioner is authorized to initiate misdemeanor proceedings before the competent court.[153] The fine imposed may not, in any case, exceed the maximum amounts that can be imposed on the controller or processor for a misdemeanor under the LPPD, i.e., up to RSD 2,000,000 (approx. €17,000).[154]

In its latest review of case law, the Commissioner highlighted several inspections initiated at the request of a data subject, which are related to the processing of personal data in the digital environment.[155] For example, in one recent case the Commissioner found that an email address containing one's forename must treated as a personal data, given that it allows for identification of a physical person.[156] In another case, the Commissioner rejected the complaint of an individual who requested that Google removes a hyperlink referring to a press article that portrays him in a negative light. The Commissioner found that the request to remove the link from the search results was not founded, since in the case at hand the interests of freedom of information outweigh the interest of personal data protection. The Commissioner emphasized the fact that the disputed article contained information on the complainant's professional life, which was of public interest.[157]

151 Report on the activities of the Commissioner for Information of Public Importance and Personal Data Protection for 2021, p. 96. [Online] Available at: https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2021/Izve%C5%A1ta2021CIR.pdf (Accessed: 15 April 2022).

152 Ibid. p. 60.

153 When the legislature prescribed pecuniary fines for misdemeanors in fixed amounts, the Commissioner is empowered to impose them directly. However, this is not typically the case.

154 Art. 95 of LPPD.

155 The Review of Case Law [Online] Available at: https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/7PublikacijaZZPL/ZZPLPublikacija_7.pdf (Accessed: 6 April 2022).

156 The Commissioner, case no. 072-16-110/2021-6, 19 February 2021.

157 The Commissioner, case no. 072-16-05/2021-6, February 19, 2021.

## 9. The digital future as a challenge for privacy

As our analysis has shown, privacy has been directly or indirectly protected in Serbian civil and criminal law for decades. However, it is the widespread use of the Internet that has truly brought attention to privacy and personal data protection issues, and led to the development of specific protection mechanisms in administrative law. Further expansion of digital technologies shall require additional legislative efforts, particularly in mass surveillance and protection of children.

Mass surveillance, which is employed to monitor a specific area, activity or person through an electronic device or system for visual monitoring, is established as a central tool of public security policy. It is expected that the use of sophisticated video surveillance platforms will continue to increase in the years to come. Further to public entities, many private sector operators are using video surveillance in their daily performance.[158] Video surveillance represents a starting point for implementing advanced technologies such as automatic number plate recognition (ANPR) and automatic facial recognition (AFR). Mass surveillance may raise concerns as to the right of privacy but also freedom of expression, which is why it needs to be properly regulated. The analysis of the LPPD reveals that in Serbia mass surveillance is not regulated by specific norms; it rather remains within the framework of general data protection provisions. For instance, the LPPD does not require that a special written decision on deployment of a video surveillance system is enacted by the controller if legal basis is not provided by the law. Also, the LPPD does not impose the publishing of a mandatory notification that video surveillance is being carried out, in a manner that enables the individual to become familiar with the implementation of video surveillance. The notification should include: (1) the identity of the controller; and (2) information on how to get informed of duration and location of storage. Finally, the LPPD does not impose any storage limitation, while the prevailing approach in comparative law is to limit the storage of data collected through mass surveillance mechanisms up to six months.[159]

One of the notable cases of abuse of video surveillance mechanisms in Serbia regards a police traffic camera which was used to zoom in on a couple having sexual intercourse in the vicinity of the Belgrade Arena, a major sports and concert hall. The video was then uploaded to pornographic websites. Another case concerned the installation of cameras in toilets of the Belgrade Bus Station, under the excuse of fear of a possible terrorist attack.[160] The cases of abuse should alert the legislature to regulate mass surveillance in a general sense, regardless of the purpose and type of controllers performing it. Clearly, in the absence of general video surveillance rules, the specific legal frameworks developed per type of controllers could be over

158 Goold, 2010, p. 39.
159 Krivokapić et al., 2021, p. 15.
160 Ibid. p. 18.

intrusive. The 2021 Initial Draft Law on Internal Affairs[161] is a drastic example of such regulatory approach. Under the 2021 Initial Draft Law, the police were authorized to undertake mass biometric surveillance in public spaces in Serbia, by means of advanced technologies equipped with facial recognition software that enable capturing and processing of large amounts of sensitive personal data in real time. Even before the start of public consultations on the 2021 Initial Draft Law, the Commissioner for Information of Public Importance and Personal Data Protection emphasized that using this type of video surveillance systems for the purpose of biometric data processing is not legal now, since there is no legal basis for such processing in the national legal framework.[162] Following the reaction of the civil sector, the Ministry of Internal Affairs withdrew the Initial Draft Law.

Another area that necessitates additional legislative and advocacy effort is that of protection of children in digital environment. Given the recent COVID-19 pandemic experience, it has become questionable whether children, as the most vulnerable group, would be adequately safeguarded in times when they are required to spend much of their time online not just for fun but for education purposes as well.[163] The national legal framework on protection of children's privacy online is yet to be completed. The LPPD prescribes that a minor, who is at least 15 years old, may independently give consent for processing their personal data in relation to information society services. If the minor is below 15 years of age, consent must be given by the parent holding the parental responsibility, i.e., a legal guardian of the minor. The controller must take reasonable measures to verify whether the consent was given by the parent (or other legal guardian), taking into consideration available technology.[164] To properly enforce these rules, several issues must be resolved. For example, all providers of information society services must establish an age verification system. Also, it should be clarified whether an education institution could give consent on behalf of its pupils for personal data processing so that the latter may access an online education tool. Furthermore, the relationship between the right to personal data processing, on the one hand, and the right to freedom of expression (including freedom to seek, receive and impart information and ideas), the right to education and the right to participate in decision-making, on the other hand, needs to be further clarified.

It seems that the authorities are aware of the need to reinforce children's privacy protection mechanisms in the digital environment, given the significant number of strategies, regulations and initiatives that are being implemented or envisaged. In 2016 the government of the Republic of Serbia adopted the Regulation

161 The Draft Law [Online] Available at: http://www.mup.gov.rs/wps/wcm/connect/c8c5d780-fcb1-46b2-96be-650dbb3ef94e/NACRT+ZAKONA+O+UNUTRASNJIM+POSLOVIMA-cir.pdf?MOD=AJPERES&CVID=nKmncZs (Accessed: April 15 2022).

162 The Commissioner, Data Protection Impact Assessment of the Use of Video Surveillance System by the Ministry of Internal Affairs, opinion no. 073-15-1741/2019-02, November 12 2019.

163 Cendić, 2020, p. 83.

164 Art. 16 of LPPD.

on Children Safety and Protection in the Use of Information and Communication Technologies,[165] which was replaced by the new Regulation[166] adopted in 2020. The regulation provides for preventive measures for protection and safety in online environment, which are supposed to be implemented through informing and educating children, parents, and teachers, as well as through establishing a place for offering advice and receiving applications related to harmful, inappropriate, illegal content and behavior online. In 2017, the Ministry of Trade, Tourism and Telecommunications established the National Contact Centre for Child Safety on the Internet (hereinafter, the NCCCSI), as the central system for applications, education, and counselling related to child safety when using digital technologies.[167] In 2020, the government adopted the Strategy for the Prevention and Protection of Children against Violence for the period 2020–2023.[168] Finally, the government published a Draft Law on the Rights of the Child and the Protector of the Rights of the Child,[169] which lays down child's right to protection of his/her personal, private and family life, including the protection of his/her home and means of communication.[170]

## 10. Concluding remarks

Digital transformation has created a situation of severe tension between the right to privacy and the extensive (personal) data pooling on which the digital economy is based. To preserve at least some aspects of citizens' privacy online, the national legislatures need to react promptly and amend the rules when needed. As our analysis has shown, within the Serbian legal framework privacy enjoyed civil and criminal law protection for decades. However, the privacy-related case law remained rather scarce up until the appearance of the Internet, which drastically increased the number of privacy breaches. Most privacy breaches in the digital environment are dealt with under administrative law framework, in proceedings before the Commissioner for Information of Public Importance and Personal Data Protection. Very few of them are resolved in civil or criminal court proceedings. The analysis of the Serbian legal framework revealed two areas in which additional legislative efforts are required, those of mass surveillance and protection of children

165 Official Journal of the Republic of Serbia 61/16.
166 Ibid. 13/20.
167 NCCCSI web-portal [Online] Available at: https://pametnoibezbedno.gov.rs/kontakt-centar/ (Accessed: 17 April 2022).
168 Official Journal of the Republic of Serbia 80/20.
169 Draft Law [Online] Available at: https://www.paragraf.rs/dnevne-vesti/070619/070619-vest15.html (Accessed: 17 April 2022).
170 Art. 20 of Draft Law.

in the digital environment. However, one should not expect that online privacy breaches can be dealt with only by way of proper and timing legislative action. The best approach would be to combine the enforcement of appropriate legal framework with upgrading of the citizens' digital literacy. Such digital literacy should at least include knowledge about economic interests in data collection and sharing practices of all digital stakeholders, the ability to identify the specific privacy risks in online environment, and knowledge about how to implement preventive data protection strategies.

# Bibliography


Božović, N. (2020) 'Biblija i ljudska prava' [Bible and Human Rights] in Božović, N., Tatalović, V. (eds.) *Evropa i hrišćanske vrednosti: Putevi Biblijske recepcije* [Europe and Christian Values: Biblical Reception]. 1st edn. Belgrade: Pravoslavni bogoslovski fakultet Univerziteta u Beogradu and Konrad Adenauer Stiftung, pp. 51–71.

Cendić, K. (2020) 'Children's Rights to Privacy in Times of Emergency: The Case of Serbia in Relation to Internet Education Technologies', *Global Campus Human Rights Journal,* 4(1), pp. 68–90.

Delany, H., Carolan, E. (2008) *The Right to Privacy – A Doctrinal and Comparative Analysis*. Dublin: Thomson Round Hall.

Delić N. (2022) *Krivično pravo – posebni deo* [Criminal Law – Special Part]. Belgrade: Faculty of Law of the University of Belgrade.

Dimitrijević, V., Paunović, M., Đerić, V. (1997) *Ljudska prava* [Human Rights]. Belgrade: Beogradski centar za ljudska prava.

Goold, B. (2010) 'How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy' in Schartum, D.W. (ed.) *Overvåking i en rettsstat – Surveillance in a Constitutional Government*. 1st edn. Bergen: Fagbokforlaget, pp. 38–48.

Greze, B. (2019) 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives', *International Data Privacy Law,* 9(2), pp. 109–128 [Online]. Available at: https://doi.org/10.1093/idpl/ipz003 (Accessed: 12 October 2022).

Jaeger Junior, A., Cravo, D.C. (2021) 'The extraterritoriality of the right to data portability: Cross-border flow between the European Union and Brazil' in Cunha Rodrigues, N. (ed.) *Extraterritoriality of EU Economic Law.* 1st edn. Cham: Springer, pp. 359–370; https://doi.org/10.1007/978-3-030-82291-0_17.

Kokott, J., Sobotta, C. (2013) 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law,* 3(4), pp. 222–228 [Online]. Available at: https://doi.org/10.1093/idpl/ipt017 (Accessed: 12 October 2022).

Krivokapić, Đ., Krivokapić D., Adamović J., Stefanović, A. (2021) 'Comparative Analysis of Video Surveillance Regulation in Data Protection Laws in the Former Yugoslav States', *Journal of Regional Security,* 16(1), pp. 5–26 [Online]. Available at: https://doi.org/10.5937/jrs16-27170 (Accessed: 12 October 2022).

Masur, P.K. (2020) 'How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information', *Media and Communication,* 8(2), pp. 258–269 [Online]. Available at: https://doi.org/10.17645/mac.v8i2.2855 (Accessed: 12 October 2022).

Midorović, S.D. (2019) 'Pravo na brisanje podataka o ličnosti dostupnih na internetu' [The Right to Erasure of Personal Data available on the Internet], *Zbornik radova Pravnog fakulteta u Nišu,* 58(84), pp. 281–306 [Online]. Available at: https://doi.org/10.5937/zrpfn0-22953 (Accessed: 12 October 2022).

Mitrović, M. (2020) 'Sloboda izražavanja i zaštita podataka o ličnosti na internetu: perspektiva internet korisnika u Srbiji' [Freedom of expression and personal data protection on the Internet: Serbian Internet users' perspective], *Communication and Media,* 15(47), pp. 5–34 [Online]. Available at: https://doi.org/10.5937/cm15-28316 (Accessed: 12 October 2022).

NOVIK, B. (2002) 'Analysis of The Fundamentals of Social Conception of the Russian Orthodox Church', *Occasional Papers on Religion in Eastern Europe,* 22(5), [Online]. Available at: https://digitalcommons.georgefox.edu/ree/vol22/iss5/2 (Accessed: 12 February 2022).

OOSTVEN, M., IRION, K. (2018) 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' in BAKHOUM, M., CONDE GALLEGO, B., MACKENRODT, M.-O., SURBLUTÉ-NAMAVIČIENÉ, G. (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?.* 1st edn. Berlin: Springer, pp. 7–26; https://doi.org/10.1007/978-3-662-57646-5_2.

PAJTIĆ, B., RADOVANOVIĆ, S., DUDAŠ, A. (2018) *Obligaciono pravo* [Law of Obligations]. Novi Sad: Pravni fakultet u Novom Sadu.

PEROVIĆ, S. (ed.) (1983) *Komentar Zakona o obligacionim odnosima* [Commentary of the Law on Contracts and Torts]. 2nd edn. Belgrade: Savremena administracija.

SEKULIĆ, M.B., GRUJIĆ, G. (2020) 'Krivičnopravna zaštita ličnih podataka' [Personal Data Protection from the Criminal Law Perspective], *Glasnik Advokatske komore Vojvodine*, 92(3), pp. 347–378 [Online]. Available at: https://doi.org/10.5937/gakv92-26404 (Accessed: 12 October 2022).

VAN DER SLOOT, B. (2017) 'Legal fundamentalism: Is data protection really a fundamental right?' in LEENES, R., VAN BRAKEL, R., GUTWIRTH, S., DE HERT, P. (eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures.* 1st edn. Cham: Springer, pp. 3–30; https://doi.org/10.1007/978-3-319-50796-5_1.

VODINELIĆ, V. (2014) *Građansko pravo: Uvod u građansko pravo i opšti deo građanskog prava* [Civil Law: Introduction to Civil Law and General Principles of Civil Law]. Belgrade: Pravni fakultet Univerziteta Union and Službeni glasnik.

WESTIN, A.F. (1967) *Privacy and Freedom.* New York: Atheneum.

Chapter VII

# The Right to Privacy in the Digital Age in the Czech Republic

David Sehnálek

## 1. Introduction

This chapter aims to introduce the issue of the protection of the right to privacy in Czech law. The starting point is the regulation of the right to privacy at the constitutional level, which I will follow with a description and analysis of the regulation in the most important Czech statutes that regulate the issue of privacy protection. With necessary exceptions, I will not address the GDPR[1] as I aim to introduce the foreign expert to those areas of Czech law that concern privacy protection but have not yet been affected by unification tendencies at the level of EU law.[2]

The content of this chapter is adapted to this objective, as it provides primarily an overview of the Czech legislation the descriptive method is the prevailing method, and the chapter has a format of a national report.

To achieve the aim of the chapter, I will analyze the right to privacy in a narrow sense, focusing only on those issues that are related to modern digital technologies and their impact on privacy protection.

1 In Czech legal science, the issue of privacy protection in the context of the GDPR is addressed by a number of authors, primarily by Jakub Míšek, and I therefore refer to his work; Míšek, 2017, pp. 331–346; Míšek, 2020; Míšek, Kasl, and Loutocký, 2020, pp. 289–293; Míšek and Bartoš, 2020, pp. 145–174; Míšek, 2014a, pp. 69–84; Míšek, 2014b, pp. 3–74; Míšek, 2014c, pp. 227–229.

2 In the Czech Republic, the GDPR has been supplemented and implemented by Act No. 110/2019 Coll., the Act on the Processing of Personal Data. This act will also not be the subject of examination in this chapter.

David Sehnálek (2023) The Right to Privacy in the Digital Age in the Czech Republic. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 235–272. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_7

Since an understanding of the legislation is not possible without considering the case law, as it is the case law that provides the comprehensive knowledge, I explain and demonstrate the issue using the case law of the Czech Constitutional Court and the Supreme Court. Both courts also work with the case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU). I will not reflect on the case law of these institutions as it goes beyond the purely national scope of the issue.[3]

The first five sections are devoted to the general issues of the right to privacy in Czech law, on the structure, wording, values, and system. Subsequent chapters are more specific and problem oriented. Here, I have chosen areas where there is case law of Czech courts that is directly related to the issue—my aim is to present law in action and not just the law in statutes, commentaries, and scientific articles. One of the starting hypotheses of this publication could be "privacy protection is regulated in the same way in all the countries concerned." The answer to this question can then be provided either by simply comparing the texts of constitutions and statutes, which are likely to be very similar. However, the approaches taken by individual national courts to interpreting these provisions may differ quite significantly. It therefore makes sense to present not only the text of the legislation but also how it has been interpreted and applied by the courts. The chosen areas then reflect those problems that have been addressed by the Czech courts.

## 2. Overview and systematics of the regulation of the right to privacy at the constitutional level

The current Czech constitutional legislation on privacy protection was adopted in connection with the division of the former federal Czechoslovak Republic. It is contained in several articles of the Czech Charter of Fundamental Rights and Freedoms of the Czech Republic (Czech Charter). The international and EU regulation on this issue is significant and present in the Czech judicial practice. The influence of the German Constitutional Court is also not negligible. Nevertheless, these external sources will not be addressed as they fall out of the scope of the research.

The regulation of privacy protection in the Czech Charter is fragmented and, therefore, quite complicated. The general protection of this right is ensured by Art. 7(1) of the Charter: "The inviolability of the person and his privacy is guaranteed. It may be restricted only in cases provided for by law." The very essence of the right to privacy protection is addressed in Art. 10(1) of the Czech Charter: "1. Everyone has the right to have his human dignity, personal honor, reputation, and

3 In Czech legal science the case law of the ECtHR and subsequent related case law of the Constitutional Court addressed in publication Bónová, 2022, pp. 157–225.

name preserved. 2. Everyone has the right to protection from unwarranted interference with his private and family life. 3. Everyone has the right to protection against the unauthorized collection, disclosure, or another misuse of personal data." Partial protection of privacy is ensured by Art. 12 of the Charter, which states that a person's dwelling is inviolable. Art. 13 of the Czech Charter states that no one may violate the confidentiality of letters or the confidentiality of other papers or records. In a broader sense, the provisions that ensure privacy protection may also include Art. 15 of the Czech Charter, which guarantees freedom of thought, conscience, and religion.

This fragmented concept of privacy protection in Czech law results from political influences in the legislative process. The original draft of the Czech Charter did not include privacy protection at all. It only guaranteed personal inviolability. Subsequently, Art. 7 of the Czech Charter added that the person's right to privacy would also be guaranteed. In parallel, it was also proposed to add to Art. 10(2) of the Charter the protection of private and family life, with the addition of Art. 7 of the Czech Charter being removed. However, the removal did not take place, the reason being the concern that "if the article on the inviolability of privacy is not there, it becomes very questionable what constitutes an unwarranted interference with private and family life within the meaning of the newly adopted Art. 10(2) of the Czech Charter."[4]

Consequently, the legal relationship between the various provisions of the Czech Charter remains unclear. In Prof. Filip's[5] opinion, Art. 7(1) of the Czech Charter is *lex generalis* to the other provisions of the Czech Charter.[6] These provisions contain some specific guarantees; they do not form an exhaustive list but only a regulation of those rights most frequently violated in the past.[7] This approach reflects the legislature's intention and is also supported by the decision-making of the constitutional court in some of its decisions.[8]

There is also a second possible approach to the systematics of the regulation of the right to privacy in the Czech Constitution. According to this approach, Art. 7(1) of the Czech Charter applies only to the *physical and mental integrity of the person*. Therefore, it is not a general clause but a particular and substantively limited provision. The right to privacy is primarily protected in Art. 10 of the Czech Charter. As a result, the two provisions overlap in the case of the processing of personal data obtained through interference with physical and mental integrity, e.g., genetic information, results of a chemical analysis of blood, etc.,[9] as not Art. 7, but also the Art. 10 deals with this issue in its third section. This approach is also supported by

4 Langášek, 2012, p. 186.
5 Prof. Filip is a constitutional lawyer and a judge of the Constitutional Court.
6 Filip, 2011, p. 14.
7 Molek, 2017, p. 295.
8 II.ÚS 770/06.
9 Langášek, 2012, p. 187.

the case law of the Constitutional Court[10] and seems to prevail, even if it does not correspond to the original intention of the legislature. However, it is supported by the system of the Czech Charter, which ranks fundamental rights according to their importance.[11]

The recent decision of the Constitutional Court concerning collecting biological DNA samples has shed light on the relationship between the two provisions of the LZPS.[12] It shows that Art. 7(1) of the Czech Charter indeed protects only the physical and mental integrity of a person. It, therefore, protects privacy in the narrow sense. Art. 10 protects privacy in a broader sense, i.e., against unwarranted interference with private life and against the unauthorized collection, disclosure, or another misuse of personal data, the so-called right to informational self-determination. The Constitutional Court, therefore, favored the first approach.

The Constitutional Court further emphasizes a holistic approach to the issue of privacy protection:

> When interpreting the individual fundamental rights, which are a representation of the right to privacy in its various dimensions as set out in the Charter, it is necessary to respect the purpose of the generally understood and dynamically evolving right to privacy as such, or to consider the right to private life in its contemporary integrity.[13]

Unsurprisingly, the Czech Charter does not give a legal definition of privacy nor defines the right to privacy. Of little to no importance is the fact that Art. 10 of the Czech Charter does not use the term "*right to privacy*," as it refers to the "*right to private (and family) life*."[14]

The Constitutional Court takes a dynamic approach to the content of this right. In its decision II. ÚS 517/99, the Constitutional Court stated:

> The right to protection of personal privacy is the right of a natural person to decide at his or her own discretion whether, or to what extent and in what manner, the facts of his or her personal privacy should be disclosed to other subjects, and at the same time to defend (resist) against unjustified interference in this sphere by other persons. The overemphasis on the positive component of the right to protection of private life leads to an inadequate narrowing of protection to the mere fact that the facts of a natural person's private life should not be disclosed to the public without his or her consent or without reason recognized by law, so that the integrity of the inner sphere, which is essential for the favorable development of the personality, is not undermined. The Constitutional Court does not share this narrow conception

10 IV. ÚS 774/18.
11 Nechvátalová, 2021, p. 225.
12 Pl. ÚS 7/18.
13 Pl. ÚS 24/10.
14 Inspiration was most likely drawn from the text of the European Convention on Human Rights.

> since respect for private life must include, to some extent, the right to form and develop relationships with other human beings. Respect for private life so conceived involves an obligation on the part of the State to act in a way that enables those relationships to develop normally.[15]

Based on this approach to the protection of private life, "the Constitutional Court extended privacy protection to the area of modern technology."[16] This extension happened in a dispute concerning the possibility of exemption from court fees in the case of an indigent person—a disabled retiree who, in the opinion of the general court, was paying excessive Internet fees and therefore had the money to pay the court fees. More precisely, she would have had it if she had not spent it on the Internet. The Constitutional Court disagreed with this approach, stating that

> in assessing the customary or justified nature of the expenditure, objective factors must also be considered; these include, inter alia, technological developments (e.g., mobile phones, the Internet) and the related changes in the methods of communication, obtaining information, dealing with the authorities, association, etc., or the development of technologies through which the individual's right to personal development, relations with other people and the outside world, i.e., the right to private life, is realized.[17]

This approach is an example of the evolutionary approach to the concept of the right to privacy in the Czech Charter and the related case law of the Constitutional Court. The Constitutional Court based its solution on the fact that "in interpreting the various fundamental rights, which are captures of the right to privacy in its various dimensions as set out in the Charter, it is necessary to respect the purpose of the generally understood and dynamically evolving right to privacy as such, or to consider the right to privacy in its contemporary totality." However, this approach must be carefully balanced by resistance to change.[18] Indeed, the driver of change should not primarily be the courts but the legislature.[19] Unfortunately, in information technology, the latter may find it challenging to keep up.

The absence of specific definitions, the general concept of this right in the Czech Charter,[20] and the dynamic approach to its text, has undeniable advantages. Indeed,

15 II ÚS 517/99.
16 Molek, 2017, p. 295.
17 Pl. ÚS 24/10.
18 Kokeš, 2012, p. 331.
19 In the decision Pl. ÚS 45/17, the Constitutional Court emphasizes the legislature's obligation to follow current events.
20 Former constitutional judge Eliška Wagnerová understands the right to privacy to serve, "along with the right to autonomy of the will, as general, overarching clauses that ensure "limitless" protection of liberty as a right even in cases not covered by specific fundamental rights." Wagnerová, 2012, p. 278.

there is no need for legislative changes at the level of constitutional law, despite the rapid development of technology. The evolution of legislation is taking place at the sub-constitutional level. At the same time, the Czech Charter provides ample scope for reflecting these changes through interpretation. The negative consequence, however, is that the shaping of the content of the right to privacy at the highest constitutional level involves a small number of unelected people—the judges of the Constitutional Court, who themselves have different views on how things should be dealt with.

Of relevance to this study is the part of the right to privacy related to *informational self-determination*. In the Czech legal system, it is regulated in Art. 10(3) of the Czech Charter and implies the possibility for an individual to make decisions about him- or herself.[21] However, the problem with modern technologies is that they are attractive to their users, easily accessible, and yet difficult to understand. One may therefore find oneself in the position of a boiling frog. Indeed, the gradual loss of privacy because of "paying with private data" in cyberspace is not apparent. Therefore, an individual has *de iure* the right to informational self-determination, but *de facto* is unable to appreciate and take advantage of this right. He may not be aware of the extent of the data transmitted, nor of the danger he may face.

It has been stated above that the Constitutional Court emphasizes the importance of the Internet and other technologies and sees them as part of the space for individual self-realization. However, this carries the risk of losing one's privacy to a massive, previously unthinkable extent. We are sharing our sensitive data with other individuals, they collect them typically for commercial reasons, and they do so usually in accordance with the law. An equally common motive for intrusion into one's privacy is to enrich oneself through illegal activity. Similarly, states use modern technologies to limit an individual's privacy. The reasons may vary from security (prevention and punishment of crime, prevention of property damage and conflicts—typically by monitoring public spaces or using cameras in common areas of houses, data retention[22]), economic (the much-discussed introduction of EET,[23] operation of electronic vignettes, value-added tax reporting[24]) or practical (introduction of electronic health books or e-prescriptions, registration) or tracing infected persons during the COVID-19 pandemic.

In this view, privacy interests conflict with prima facie countervailing security, commercial and other interests. It might therefore appear at first sight that, as a legislature or a judge, we must choose between protecting one value or the other as both are not possible at the same time. But this view would not be correct. Indeed, by setting up appropriate oversight and regulation, both can be achieved at the same time.[25]

21 Pl. ÚS 24/10.
22 Pl. ÚS 24/10 and Pl. ÚS 45/17.
23 Pl. ÚS 26/16.
24 Pl. ÚS 32/15.
25 Solove, 2011, p. 2. https://ssrn.com/abstract=1827982 (Accessed: 22 June 2022).

As the right to privacy is not absolute, the law can limit it.[26] The trend of developing and shaping the right to privacy in the Czech Republic is well reflected in the Data Retention II decision. In it, the Constitutional Court states:

> Along with the growing threat of terrorist attacks, a logical trend has developed to strengthen the powers and tools of public investigative authorities at the expense of maintaining the existing standard of fundamental rights of individuals. However, this trend is gradually changing over time, and also as a result of decisions of the Constitutional Courts, the ECtHR, or the CJEU, political representations are beginning to understand the need to find a balance whereby States can effectively and efficiently fulfill their positive obligations without interfering more than is strictly necessary in a democratic society with the fundamental rights of individuals, in this context, in particular, the right to privacy and informational self-determination under Art. 10(2), (3) and Art. 13 of the Charter. The change in the trend towards strengthening the protection of personal data, or rather redressing the lost balance, is demonstrated, inter alia, by the adoption of the GDPR or the preparation of the adoption of the so-called e-privacy Regulation, regulating the area of privacy and electronic communications instead of the existing directive of the same name. The rapid development of information technology cannot be stopped or slowed down by any legislation; the reach of the Internet and other networks enabling electronic communication is not limited to national borders but is a global phenomenon, a worldwide phenomenon that national legislatures deal with it in different and difficult ways. It is necessary to deal with the fact that a plethora of different data (metadata) is being generated by the active involvement of individuals, and the risk of its misuse is increasing exponentially—the means of protecting personal data must be adapted to this. The Constitutional Court has concluded that in the conditions of today's information society, in which the average individual uses electronic communication services at almost every step and voluntarily accepts that quantum amounts of data are stored about him, it would be unwise to tolerate a situation in which service providers have users' data, and the state apparatus (in justified cases) does not. The blanket retention of traffic and location data represents an effort by the State to keep pace in the information society and have effective tools to carry out its tasks—here in particular in security of the State and its citizens.[27]

The decision shows a certain degree of *resignation to a high level of privacy protection.* This is contrary to trends at the EU level. It is being done so just in favor of the public authorities, for purely factual reasons, and moreover, for reasons caused by the private sphere. At the same time, the factual situation is perhaps overemphasizing the question of the extent to which the storage of individual data is voluntary. Regarding

26 However, even the law cannot exceed the limits set by the Constitution and the Czech Charter. Art. 7 of the LZPS prohibits torture or cruel, inhuman, or degrading treatment or punishment.

27 Pl. ÚS 45/17 34.

trends at the EU level, the Constitutional Court monitors and respects the external legal environment. The standards of privacy protection contained in the EU Charter of Fundamental Rights and the European Convention, and consequently also in the case law of the ECHR and the CJEU, are routinely used and cited in its decisions.

## 3. Overview and systematics of the regulation of the right to privacy at the sub-constitutional level

At the sub-constitutional level, the right to privacy is regulated in private law primarily by Act No. 89/2012 Coll., the Civil Code. This statute regulates in Arts. 81 to 91 the protection against the dissemination of likenesses and the protection against invasion of privacy in accordance with the Czech Charter.[28] Protection is thus granted only to natural persons. At the same time, the Civil Code contains provisions on exceptions—official licenses, based on which interference with this right is permissible.

The protection of the privacy of legal persons is provided for in Art. 135 of the Civil Code.[29] Case law on this provision regarding the privacy of legal persons does not yet exist.[30] At the same time, Prof. Dvořák, author of the commentary on this provision, asks the question of how the privacy of a legal entity can be interfered with at all if it is a simple fiction. He also argues that the protection of privacy in this provision is a legislative technical error, something that the legislature did not intend to regulate at all.[31] Therefore, it can be concluded that although there is a legislative space for the protection of the privacy of a legal person, it has not yet been filled by practice and legal theory does not yet know how to deal with it.[32] Within the sphere of civil law, specific regulation of the right to privacy is secured by the Act No. 262/2006 Coll., the Labor Code in labor legal relations.

In administrative law, the protection of the right to privacy is ensured by Act No. 127/2005 Coll. on electronic communications, as amended, Act No. 181/2014 Coll. on cybersecurity, Decree No. 82/2018 Coll. on cybersecurity, and several other

28 The value significance of the right to privacy is generally emphasized by its mention in Art. 3, para. 2 of the CC.

29 This provision states: "(1) A legal person which has been affected by having its right to a name disputed or which has suffered harm due to unlawful interference with that right, or which is under threat of such harm, in particular by unauthorized use of the name, may claim that such unlawful interference be refrained from and its consequence remedied. (2) A legal person enjoys the same protection against anyone who, without a lawful reason, interferes with its reputation or privacy, unless for artistic or scientific purposes or for print, radio, television or similar coverage; however, neither such an interference may be in conflict with the legitimate interests of the legal person."

30 More precisely, I am not aware of its existence, and leading commentaries do not mention it either.

31 Dvořák, 2014, p. 461.

32 Lasák in another Czech commentary does not discuss nor question the privacy of legal persons at all. Lasák, 2014, p. 713.

regulations address the right to privacy to some extent. In the healthcare sector, privacy is regulated by the requirement of confidentiality in relation to healthcare services. This regulation is contained in Act No. 372/2011 Coll. on Health Services and Conditions of their Provision.

In criminal law, the protection of privacy is provided for in Act No. 141/1961 Coll., the Criminal Procedure Act, in Articles 180 to 184, which regulates Criminal Offences against Rights for Protection of Personality, Privacy, and Secrecy of Correspondence. Specifically, the following offenses are regulated: Illicit Disposal with Personal Data,[33] Infringement of Rights of Another,[34] Breach of Secrecy of Correspondence,[35] Breach of Confidentiality of Files and other Private Documents,[36] and Defamation.[37] The Criminal Law further protects against cyberstalking.[38]

The two procedural rules governing evidence are also relevant to the protection of privacy. In the area of civil law, evidence taking is regulated by Act No. 99/1963 Coll., the Code of Civil Procedure, which does not contain any special provisions specifically addressing privacy protection in the context of digital technologies. In the area of criminal law, the issue is regulated by Act No. 141/1961 Coll. on Criminal Procedure. This Act regulates the protection of privacy both through general institutes and through newly adopted provisions that consider modern technologies. Specific provisions of this law regulate the interception and recording of telecommunications[39] and further surveillance of persons and items during which any audio, visual or other records shall be made.[40]

## 4. Privacy and modern technologies in the civil law of the Czech Republic – General remarks

The Civil Code enshrines the protection of privacy in its Art. 3, according to which

> Private law protects the dignity and freedom of an individual and his natural right to pursue his own happiness and the happiness of his family or people close to him in a way that does not unreasonably harm others. (2) Private law rests in particular on

33 Art. 180 of the Criminal Code.
34 Art. 181 of the Criminal Code.
35 Art. 182 of the Criminal Code.
36 Art. 183 of the Criminal Code.
37 Art. 184 of the Criminal Code.
38 Art. 354 of the Criminal Code.
39 Art. 88 of the Code of Criminal Procedure.
40 Art. 158d of the Code of Criminal Procedure.

> the principles that (a) everyone has the right to the protection of his life and health, as well as of his liberty, honor, dignity, and privacy.[41]

From a systematic point of view, the quoted provision is, as far as the right to privacy is concerned, a simple repetition of what is already contained in the Charter. The cited Regulation contained in the Civil Code, therefore, does not constitute any added value since it does not extend or further specify the general constitutional framework in any way but merely repeats it.[42] The quoted provision elevates the protection of privacy to a *principle*, but in reality, the protection of privacy is a *value* and the intention of its protection as *a policy*.[43] The significance of the quoted provision can therefore be seen only in the fact that it emphasizes the legislature's interest in protecting this value and presupposes its horizontal application in Czech civil law by the courts and the addressees of this legislation.

The protection of privacy is ensured in Czech private law by means of the general clause of protection of personality rights and the specific provisions of the Civil Code. According to the general clause contained in Art. 81 of the Civil Code, "The personality of a person, including all his natural rights, is protected. Everyone is obliged to respect a person's free decision to live according to his own." This general provision is followed in the same clause by a demonstrative enumeration of human values, according to which "the life and dignity of the human being, his health and right to live in a favorable environment, his dignity, honor, privacy and his expressions of his personal nature shall, in particular, enjoy protection." Human privacy is specific among these values in that a violation of any other value that is protected by the cited provision will also result in an invasion of privacy.[44]

The regulation of privacy protection is further specified by the Civil Code in the provisions of Art. 84 to Art. 90. These provisions build on the general clause and are included in subsection 2 of the Civil Code, entitled *Likeness and Privacy*. The two interrelated rights are therefore regulated together. The protection of privacy is primarily provided for in Art. 86 of the Civil code. According to this provision,

> no person shall invade the privacy of another unless he has a lawful reason to do so. In particular, one may not, without a person's consent, invade his or her private premises, monitor his or her private life or make audio or visual recordings of it, or use such or other recordings made of a person's private life by a third party, or disseminate such recordings of his or her private life. Private writings of a personal nature shall be protected to the same extent.

41 Art. 3 of the Civil Code.
42 See Pelikán and Pelikánová, 2014, p. 25.
43 Ibid.
44 Ondřejová, 2016, p. 199.

It is clear from the text of this provision that the right to privacy has *erga omnes* effect. At the same time, this right may be limited by law and is therefore not absolute. The following provisions of the Civil Code provide for limitations (so-called *statutory licenses*). These permissible limitations overlap with those provided for in the data protection regulations.[45] Restrictions are possible where *consent is given* to interfere with the right to privacy,[46] in the case of an official license, i.e., to protect one's own rights or the rights of a third party,[47] and for scientific or artistic purposes and for press, radio, television, or similar reporting.[48]

Of course, the legislation does not preclude the granting of consent to the interference with the right to privacy (principle of autonomy). This possibility is often used in cyberspace. Personal data is commonly used as a form of consideration for services provided or as a prerequisite for a discount on the normal price of services or goods.

Consent should be given in advance, knowingly and transparently. It may be hard to meet these requirements in cyberspace for two reasons. First, in an electronic environment, it is relatively easy to "hide" consent among other provisions, thereby making it "invisible." Second, people often do not carefully read the contracts they enter online. While the first practice is legally solvable, especially in the case of consumers, the second situation does not have an easy solution. On the other hand, rights belong to the vigilante, and the law should not be overly paternalistic.

It follows from the above that consent to an interference with the right to privacy is necessary in some cases under the Civil Code. Consent to the processing of personal data is also foreseen and required by the GDPR. There is to some extent an overlap between privacy and data protection. In case of such overlap, only one consent is fully sufficient. The parameters of consent are not explicitly defined by the Civil Code, therefore the general and rather lenient rules governing legal conduct apply. The GDPR, on the other hand, defines the scope, form, and other elements of consent quite precisely. In view of this fact, I therefore conclude that in the case of consent granted based on the GDPR which meets the strict criteria set by this act, the conditions required by the Civil Code are also fulfilled and no other action is needed.

Any ill-considered or unintended consent is legally solvable. It is also possible to change your mind and reconsider previously granted consent. The provision of Art. 87 of the Civil Code allows for the *unilateral withdrawal of consent already given*. This possibility is even available if the consent has been granted for a fixed period. The provision is mandatory. The possibility of withdrawing consent already granted cannot, therefore, be excluded even by mutual agreement of the parties.

Withdrawal of the consent granted for a fixed period may constitute a serious interference with the right of the other party. The Civil Code, therefore, provides

45 Nonneman, 2012, p. 508.
46 Art. 87 of the Civil Code.
47 Art. 88 of the Civil Code.
48 Art. 89 of the Civil Code.

that if this is done "without a material change in circumstances or other reasonable cause, the person revoking the consent shall compensate the person to whom the consent was given for the damage resulting therefrom."[49] This opens the way for compensation in the case where consent is tied to a certain consideration, this is consumed, and consent is subsequently revoked on purpose.

The possibility of withdrawing consent looks easy and unproblematic at first sight. Legally, it is. In practice, however, misunderstandings arise. I can demonstrate such a problem by the hoaxes that periodically appear and spread on Facebook.[50] The gist of one of them (including various sub-variants) is that the persons whose privacy is at stake must share a text in which they explicitly do not give Facebook their consent to use what they themselves have previously shared. In this case, however, consent is a condition of the use of the service as by creating a Facebook account, and a customer enters into a contract which is the legal basis for personal data processing. Therefore, withdrawal of consent cannot be made unilaterally in a situation where the service is still being used. To make such a change, it would also be necessary to change the content of the contract, i.e., to renegotiate it with Meta, the company that operates Facebook, which is not very likely.[51] It appears that many of the recipients of the legislation do not understand how the law works (see the references to the Berne Convention in the hoax quoted above), nor do they understand the basic concepts. Sharing such hoaxes, on the other hand, reveals a great deal about the people who share them.

Of legal significance is the question of how to proceed in situations where consent to interference with the right to privacy is lacking. Modern technology makes it possible, to a degree previously unthinkable, to make a video or audio recordings of people without their knowledge. Given the continuing miniaturization, it is also increasingly unlikely that the making of such recordings will be detected by those being recorded.

49 Art 87, para. 7 of the Civil Code.

50 The text of one of the variants reads, "As of January 3rd, 2015 at 3:30 p.m. Central standard time. I do not give Facebook or any entities associated with Facebook permission to use my pictures, information, or posts, both past and future. By this statement I give notice to Facebook it is strictly forbidden to disclose, copy, distribute or take any other action against me based on this profile is private and confidential information. The violation of privacy can be punished by law (UCC 1-308-11 308-103 and Rome statute). NOTE: Facebook is now a public entity. All members must post a note like this. If you prefer, you can copy and paste this version. If you do not post this statement at least once it will be tactically allowing the use of your photos, as well as information contained in the profile status updates. DO NOT SHARE you MUST copy and paste this… I will leave a comment so it will be easier to copy and paste!!!" [Online] Available at: https://www.lupa.cz/clanky/facebookovy-hoax-s-pravy-k-prispevkum-se-vraci/ (Accessed: 07 September 2022).

51 For the sake of completeness, I would like to add that Meta is thus entitled, pursuant to Art. 6, para. 1b of the GDPR, to process only the personal data necessary for the performance of a contract. The customer's consent will nevertheless be required for further processing and further services. However, the eventual revocation of such consent cannot technically be done in the manner suggested in the hoax. The revocation was not, at least under Czech law, properly served the other party.

From a practical point of view, the significance of interference with another privacy is that it may enable things to be proved that would otherwise be impossible to prove. One is often more likely to say things in private that one would not say in public, and one is also more likely to speak plainly, truthfully, and openly about what one thinks. In such a situation, the rules in procedural law that courts should decide based on truth[52] collide with the substantive rules protecting privacy. Solutions to this problem in Czech law will be introduced below.

## 5. Instruments of enforcement of the right to privacy in Czech private law

Under Czech law, the right to privacy is not *time-barred*. However, this does not apply to rights to compensation for harm caused to these rights.[53] The general statute of limitations in Czech law is three years, so it is necessary to bring an action to court within this period.[54] The person concerned has the right to claim that the unlawful interference is refrained from or its consequences remedied.[55]

The invasion of an individual's privacy by modern digital technologies can have far-reaching and difficult-to-remedy consequences. The publication of defamatory text, photographs, videos, or other recordings can affect the psyche of a person, especially a young, developing person, in a severe and irreversible way. The legislation, therefore, provides for the possibility that even *non-pecuniary harm* caused in this way is compensated by appropriate satisfaction. Satisfaction must be provided in money unless real and sufficiently effective satisfaction for the harm incurred can provide for satisfaction otherwise.[56] It follows from the above that monetary compensation is only a secondary instrument of compensation for the injured person in the Czech law. The primary one would be, for example, a public apology, or a withdrawal of problematic information. However, such a solution will not always be an option either. Furthermore, the Czech Civil Code also explicitly provides for the possibility for the injured party to claim *compensation for the mental distress caused*.[57]

As the act of interfering with an individual's privacy may also have an impact on other persons (e.g., the parents of a child who has been affected by interference

52 Czech civil litigation is based on the principle of formal truth. The principle of substantive truth, and thus the accurate determination of the facts, is important in civil non-contentious proceedings and in the area of administrative and criminal proceedings.
53 Art. 612 of the Civil Code.
54 Art. 629, para. 1 of the Civil Code.
55 Art. 82 of the Civil Code.
56 Art. 2951, para. 2 of the Civil Code.
57 Art. 2956 of the Civil Code.

with privacy on the Internet), the Czech law also provides for the possibility of also compensating these third persons.[58]

Finally, Czech law also protects against someone else's enrichment by interfering with one's right to privacy. In such a case, the injured party may claim: 1) that an enriched person who did not act in good faith makes restitution of the entire enrichment he acquired, and 2) that he also compensates for the revenue which the impoverished person would have gained.[59] Alternatively, as compensation for the unlawful disposal of the values related to his personality rights, the impoverished person may demand twice the remuneration usual for the consent to such disposal.[60]

## 6. Privacy protection and modern technologies in Czech civil procedural law—Cases on the right to privacy and the right to a fair trial

The Czech procedural rules are set very generally, as they do not explicitly regulate the issue of electronic evidence; in my opinion, that is a good approach from the point of view of modern digital technology because the legislation is in line with the principle of technological neutrality. According to Art. 125 of the Code of Civil Procedure, "all means by which the state of the case can be established may be used as evidence." This creates an apparent conflict, as the Civil Code sets certain conditions should the interference with privacy be admissible, and these conditions may not be met (for example the consent is missing, or there is no official statutory license), whereas under the Code of Civil Procedure, no precondition in the form of the consent of the person concerned is required.

The Czech civil courts have dealt with this problem pragmatically in two ways. First, by interpretation of the terms "privacy" and "expressions of a personal nature." Second, the problem has been addressed by balancing the various interests involved. It must be stressed that the resolution of individual situations is ambiguous and the conclusions of the various courts, as well as their legal reasoning, often differ widely.

58 However, the conditions are set very strictly. See Art. 2971 of the Civil Code: "If justified by special circumstances under which the tortfeasor caused harm by an unlawful act, including, without limitation, by breaching an important legal duty due to gross negligence, or by causing harm intentionally out of a desire to destroy, hurt or for other especially reprehensible motives, the tortfeasor shall provide compensation for the non-pecuniary harm to everyone who legitimately perceives the harm as a personal misfortune which cannot be undone otherwise."

59 Art. 3004, para. 1 of the Civil Code.

60 Art. 3004, para. 2 of the Civil Code.

An example of the first solution is a situation that arose in a dispute between the partners of a commercial company. One of the partners made an audio recording of a meeting, which was subsequently used as evidence in court proceedings. In this case, both the first instance court as well as the court of appeal concluded that the taking of the recording without consent violated the individual's right to protection of personality, but the provisions of the procedural rules that all means of establishing the situation may be used as evidence in proceedings allow such evidence to be taken in proceedings before the competent public authority, as they create an official statutory license. However, the Supreme Court did not accept this reasoning and came up with a different solution. It noted that the Civil Code, in the provisions at issue, provides

> protection only for those expressions of natural persons which are personal in nature. Therefore, as a rule, speeches that occur in the exercise of a profession, in commercial or public activities do not have a personal character. The audio recording admitted in evidence by the courts in the present case is a recording of the proceedings of the shareholders of a commercial company, and this recording concerns solely the company's problems. In such circumstances, therefore, the participants' speeches in the recorded conversation cannot be regarded as being of a personal nature. It follows from the foregoing that making the sound recording in question could not have infringed the personality rights of the parties.[61]

The conclusions contained in this decision have been further elaborated in the case law of the Supreme Court. In the Czech Republic, a new Civil Code came into force in 2014, which expanded the possibilities of limiting the right to privacy. In contrast to the previous regulation, the new Civil Code also allowed the taking or use of an image or a sound or visual recording regarding the exercise and protection of other subjective private rights, generally in proceedings before a public authority and under public law. In a dispute concerning the validity of an employee's dismissal, recordings were used that captured threats made by the employee. The Supreme Court stated,

> a sound or visual recording which relates to a person or his expressions of a personal nature and which was made by a private person without the knowledge of the person recorded may be used as evidence in civil proceedings only where it is intended to lead to the proof of a fact which cannot otherwise be proved (by evidence, which does not interfere with the absolute personality rights of the person concerned), and where the other circumstances of the case lead to the conclusion that the right to protection of the personality of the person concerned cannot be given priority over

61 30 Cdo 64/2004.

> the right to a fair trial of the person who benefits from the use of evidence of an audio or visual recording relating to that person or his or her personal manifestations.[62]

In the present case, however, facts could otherwise be proved according to the Supreme Court. Witnesses were also present at the hearing. Therefore, a recording was not necessary to prove the facts. However, the important issue, in my view, is the quality and credibility of the individual pieces of evidence. Formally, the evidence is equal under Czech law, but in fact, the testimonial value of the recording may exceed that of the witness statement. A recording captures and preserves the course of events in an objective manner. In contrast, witness testimony depends on several subjective factors, including the quality of memory and the ability to reproduce what is heard (and seen).

The Constitutional Court used both methods of justification in a case involving a wrongfully dismissed employee. This employee was formally dismissed out of redundancy. However, the real reason for his dismissal was that he had complained about the company's management to its foreign owner. This was supposed to be evidenced by an audio recording, but it was made without the knowledge of the person being recorded. The Constitutional Court referred to the earlier case law of the Supreme Court (cited above). It stated that the recording was made during work and was therefore not protected in principle as a manifestation of a personal nature. However, if it did contain expressions of a personal nature, the right to a fair trial would still prevail. According to the Constitutional Court,

> in normal circumstances, the arbitrary recording of private conversations without the participants' knowledge is a gross interference with their privacy. In most cases, such a practice, which has the appearance of being insidious, is morally and legally unacceptable, especially if it is motivated by the intention to harm the person being recorded. The Constitutional Court is firmly opposed to the unfair practice of electronic surveillance and covert recording of private and professional meetings, which, as a rule, not only contravenes the law, but also, from a social and ethical point of view, spreads an atmosphere of suspicion, fear, uncertainty, and distrust in society. However, a completely different approach should be taken in cases where the secret recording of an audio recording of a conversation is part of the defense of the victim of a crime against the perpetrator or where it is a way of obtaining legal protection for a significantly weaker party to a significant civil and labor law dispute. The interference with the right to privacy of the person whose speech is recorded is fully justified here by the interest in protecting the weaker party to the legal relationship who is at risk of serious harm (including, for example, loss of employment). The provision of a single or key piece of evidence in this way is analogous to acting under conditions of extreme hardship or self-help leave. In the present case, the admission of the complainant's recording of an interview with NV, one of the

62 21 Cdo 1267/2018.

> intervener's foreign executives, in the proceedings for the annulment of his dismissal is fully consistent with the legitimate aim pursued, which is, as a matter of priority, the protection of employees and the very protective function of labor law vis-à-vis the employee in employment relationships.[63]

It can be deduced from the reasoning of the Supreme Court and the Constitutional Court that the use of evidence interfering with the right to privacy without the consent of the person concerned is an exceptional situation. Firstly, it will be admissible if there is no other way of proving the fact in question, unless the sole purpose of the recording is to harm the person being recorded. This option is always permissible, regardless of the nature of the parties concerned. Secondly, such evidence will be admissible even where there is a possibility of proving the relevant fact by other means. However, this is possible only in exceptional circumstances where the weaker party to the legal relationship in question uses such evidence as a defense. The concept of the weaker party may include not only an employee, but also a consumer, a victim of crime, and presumably the elderly, young children, seriously ill persons, etc. This form of protection, on the other hand, will not be afforded to employers, commercial companies, criminals or the Czech state and its authorities.

The case above concerned a situation, where the protection of privacy was secured primarily by the Civil Code which sets conditions and limits of this protection. On the contrary, a telephone calls between commercial companies (and their employees) falls outside the scope of the privacy protection provided by the Civil Code. Conditions and limits set by this act thus do not apply on such a situation. However, the mechanism for resolving conflicts between the right to a fair trial and the constitutionally protected right to privacy is the same as in cases, where the Civil Code applies. The Constitutional Court did come to this conclusion in a case involving a dispute between two commercial companies. The dispute concerned the admissibility of evidence in the form of a recording of a telephone conversation. The call had been monitored, so the general courts concluded that the recording was not admissible. This was because the company had only consented to monitoring, not storage of the call. On the contrary, the Constitutional Court stated:

> When the right to judicial protection is weighed against the right to privacy, the right enshrined in Art. 36(1) of the Charter must be given priority in this case. It cannot be overlooked that the communication concerned a business case between two business entities and the intervener was aware of the monitoring of the call. The purpose of taking that evidence was precisely to prove that the contract which was the subject of the call had been concluded. Therefore, it cannot be considered that this evidence was intended to interfere with the privacy of any person or to be misused for other purposes. In the view of the Constitutional Court, the taking of evidence of a recorded telephone call, the subject of which was a commercial offer, does not exceed

63 II.ÚS 1774/14.

an unacceptable degree of contextual interference with the fundamental right to privacy. In the opinion of the Constitutional Court, this is sufficient for the applicability of such evidence in court proceedings.

The case concerned a recording made in secret. However, in the course of work, situations may arise where a person is filmed without being able to defend against it. These situations typically arise during professional, commercial, or public activities. For example, a student may record a lecture by his lecturer, a citizen may record a police officer during a raid[64] or a politician during a meeting of a public authority. Similarly, recordings can also be made of persons who, although they do not hold political office and therefore cannot be considered politicians, have made a public speech at a meeting of a public authority.[65] Naturally, only what relates to the performance of *public activities* may be recorded in this way; speeches of a purely private nature relating to family, health, etc., cannot be, in principle, recorded.

## 7. Privacy protection and modern technologies in Czech law – Unsuccessful justification

While victims of crime may defend themselves against recordings that constitute an invasion to the right to privacy, even this defense has its limits. Such recordings may not be used in an "offensive manner." This problem can be illustrated by a well-known dispute which was covered by Czech media. In this case, a person who was robbed of his laptop used his IT knowledge to his advantage. The truth is, that he was essentially forced to do so by the fact that the Czech Police was unable to find the perpetrator of the theft. The robbed person gained remote access to the laptop and took pictures of the persons using the laptop and posted the pictures on the Internet. They were published together with derogatory nicknames he gave them according to the characteristic use of the laptop ("farmer," "wanker"). However, the persons concerned did not steal the laptop but bought it legally (albeit at a conspicuously low price). The dispute dragged on for many years, the problem being to determine whether the robbed IT specialist had acted legally and, if not, what damages he should compensate the persons concerned for the unwarranted invasion of their privacy. However, there was a clear agreement between the courts that the

64 See the Opinion of the Security Policy Department of the Ministry of Interior on the acquisition of police officers' signs in the performance of their duties.

65 Judgment of the Municipal Court in Prague 8 A 316/2011-47.

publication of photographs on the Internet constituted an infringement of the right to privacy.[66]

Coercive use of data that invades a person's privacy is common. As a rule, however, they infringe personal rights and not directly the privacy of the person concerned. Such behavior was also common in the days before the Internet, Facebook, etc. The Supreme Court has commented on this issue in a case concerning alleged non-payment of rent. This information was published by the property owner in a periodical he published and was presented to the public as a so-called "public criticism."[67]

Public criticism is permissible in the Supreme Court's jurisprudence in certain circumstances. However, it must not be out of proportion to the objective of the criticism. This will be the case, for example, if it implies an intention to disparage or insult the person criticized (so-called intense excess).[68] Similarly, public criticism of a person's conduct is inadmissible if the reasons which justifiably led to the conduct complained of are concealed or obscured from the critic. From this perspective, it was also legally inadmissible to publish information on the rental debt without properly explaining the context.[69]

Public criticism is frequent on social media. It is common for people and companies to post information in pursuit of their own personal gain, but also for the "public good". Indeed, just recently, I noticed on the Facebook pages of two of my friends that they independently shared similar information about a Russian soldier who was supposed to have sent his wife "loot" weighing half a ton from Ukraine. The information was accompanied by a photo of the soldier, his wife, and their family. Sharing such information without any possibility of verifying its veracity is legally problematic considering the above rules. What makes it even more piquant is that one of the sharers is a law school graduate.

Such conduct would be permissible in a situation where a person himself or herself decides to disclose certain information belonging to his or her private sphere, e.g., by posting it on Facebook or Instagram, e.g., to boast. The further sharing of this information, if it has not been altered or consent to disclosure withdrawn, would in principle no longer be subject to privacy protection.

Such conduct may also be permissible should it fall withing the concept of *citizen journalism*. Generalizing the described problem, I conclude that its core lies in the conflict between the right to privacy and the right to freedom of expression. Within

66 Pokorný, 2017, Šmírovaní uživatelé kradeného notebooku si na odškodné počkají. Soud musí případ znovu projednat [Online] Availabe at: https://zpravy.aktualne.cz/domaci/smirovani-uzivatele-kradeneho-notebooku-si-na-odskodne-pocka/r~874defd01f6211e7bc55002590604f2e/ (Accessed: June 22, 2022) and Kočí, 2011, Případ šmírujícího MacBooku — co v Televizních novinách nebylo [Online] https://www.lupa.cz/clanky/pripad-smirujiciho-macbooku-co-v-televiznich-novinach-nebylo/ (Accessed: 22 June 2022).

67 30 Cdo 4613/2007.

68 30 Cdo 2573/2004.

69 30 Cdo 4613/2007.

the framework of freedom of expression, protection is granted to all persons who are active in the field of journalism (the journalistic exception). Journalism is understood very broadly in the case law of the CJEU,[70] so that even the lawyer described above — a graduate of my alma mater — may in each case fulfill the characteristics of a *person active in the field of journalism*. However, the essential difference between the case dealt with by the CJEU lies in the fact that in this case the original source of the information was obtained illegally, the information can be made public in an alternative way, i.e., in a way that ensures the protection of the rights of the persons concerned without reducing the information value. I therefore consider the case of sharing pictures described above to be disproportionate and unlawful. In my opinion, the journalistic exception is rather inapplicable in his case.

## 8. Privacy of third persons and modern technologies in administrative and court proceedings

Special rules apply to work in the public administration. In administrative law, the possibility of making recordings of the proceedings, and thus also of the official, is not provided for directly by law. Nevertheless, in view of the constitutional principle contained in Art. 2(4) of the Constitution, every citizen may do what is not prohibited by law. No one may be compelled to do what the law may not impose. No law prohibits a party to an administrative procedure from making an audio recording of the course of an oral hearing, and it is irrelevant whether the proceedings is public or private. Therefore, there is no basis for concluding that by making an audio or visual recording of the proceedings a party is grossly disorderly and may be banned from the place of the hearing. This could only occur in a situation where, in accordance with the provisions of Art. 63 of the Act No. 500/2004 Sb. Administrative Procedure Code, taking of a recording would constitute a gross disturbance of the peace.[71]

In court proceedings, the possibility of making a recording is expressly regulated. Provision of Art. 6(3) of Act No. 6/2002 Sb. Courts and Judges Act directly provides that

> visual or audio transmissions and visual recordings may be made during a court hearing only with the prior consent of the president of the chamber or a single judge. Sound recordings may be made with the knowledge of the President of the Chamber or a single judge; the President of the Chamber or a single judge may prohibit the making of such recordings if the way they are made is likely to prejudice the conduct or dignity of the proceedings.

70 See case C-73/07 Satamedia Oy.
71 5 As 37/2009-99.

When making a recording, a situation may arise where the recording captures a person whose privacy is not guaranteed — for example, because he or she is acting within the scope of his or her employment (or business). At the same time, however, the recording may include a third party who is protected. This will be the case, for example, in a public meeting of a city council, where the recording of the meeting will capture both the politician and official as well as the public present.

The Civil Code protects not only privacy, but also the likeness of a person. Therefore, as a result "the depiction of a person's likeness in any way so that his identity can be determined from the depiction is only possible with his consent."[72] The protection is provided for situations where a person's likeness is captured, it is not relevant in what form the capture is made (thus, various technical means may be used, such as photography, film, digital recording, but also painting, graphics, etc.) and, finally, the possibility of determining the identity of a person from the depiction is provided, where the depiction of a person contains a sufficient number of characteristic features of the likeness of a particular person by which he or she can be identified as a unique and unmistakable being.[73]

In the case of recording the proceedings of a court, administrative authority, etc., from the perspective of Czech law, there is in principle no interference with their privacy, but their consent is necessary to capture their image on the recording. The solution is therefore not to record such proceedings at all, or to anonymize the recording by blurring or overlaying a substantial part of the third party's face.

Fortunately, while consent must be given, the law does not specify its obligatory form. In practice, therefore, many situations will be solvable by assuming a person's consent to the capture of his or her likeness when a person knows about the fact that the recording is being made and knowingly enters premises (public or private) that are declared as monitored (in any form — e.g., by an explicit warning or even just by visibly installed cameras, etc.).[74]

## 9. Privacy policy and audio, visual, or other recordings of an item

Protection against interference with a person's privacy is provided *solely to people*. Therefore, the publication of a photograph or video or audio recording of a thing (a house, a car etc.) will not, by its nature, generally be an invasion of privacy. The Supreme Court came to this conclusion in a case involving the publication of photographs of a house that was accompanied by the surname of the owner of the house.

72 Art. 84 of the Civil Code.
73 Pavlík, 2014, p. 324.
74 Ibid.

The Supreme Court stated that the general rule would be that

> The publication of a photograph of a house does not constitute an unwarranted interference with the personal rights of the owner of the house, namely his right to privacy, because a house is a thing that is perceptible from the outside and therefore does not belong to the sphere of personal privacy, which is the inner intimate sphere of a natural person's life necessary for his self-realization and further development.

At the same time, however, it also stated that such publication may

> possibly be an inherently inadmissible probe into the intimate sphere of a natural person, capable of illegally informing the public about his individual foundation, or focus, direction, etc.—i.e., in general, inadmissibly testifying about the private sphere of a natural person.

The above shows that context always matters. *The whole body of information that is provided and its predictive value in relation to a particular person is therefore essential*. The regulation is general, and it is therefore always for the court to make a specific assessment. This is not a criticism of the legislation; life is varied, and it is therefore not desirable for the legislation to cover every conceivable possibility.

---

## 10. Invasion of children's privacy by their parents — "Sharenting"

The development of information society services, the various social networks, has facilitated the dissemination of information that falls within the sphere of privacy. It is not usually a problem if one shares information about oneself. Part of our freedom is also the freedom to decide which part of our privacy becomes public.

The problem arises when we share information about another person. Consent can be given *ex post*, even by implied consent. This was the case, for example, with the famous hockey player Jaromír Jágr, whose lover posted a photo on social media after a night spent together.

However, the situation is different when information falling within the sphere of privacy is published by persons who have the right to do so, but which concerns another person who cannot decide for himself or herself. Typically, this will be the case for parents and children ("sharenting") and may also apply to persons deprived of their legal capacity and their guardians. More broadly, this also includes the activities of schools and nurseries that publicly share what is happening inside their institution, either by photograph or video.

Invasion of a child's privacy can occur in different ways in an online environment. Parents can use their child's identity to create a social networking profile, which they manage themselves. They can also share information, photos, or videos relating to their child through their own profile. From a privacy perspective, there is no practical difference between the two situations. Leaving aside the security risks of such behavior, as well as the moral considerations (including the impact that sharing information in the environment of the "eternal" Internet may have on their child one day in the future), there remains the problem of the permissibility of such behavior.

Czech courts have not yet resolved a dispute between a parent and a child concerning the disclosure of information about the child's life. At the same time, no specific legislation has been adopted to address this issue. Therefore, only the general legislation regulating the position of parents in the upbringing of a child is applicable. This regulation is, nevertheless, according to my opinion sufficient.

The issue is in the Czech law regulated primarily by the provision of Art. 858 of the Civil Code, according to which:

> Parental responsibility includes rights and duties of parents consisting in caring for the child, including, without limitation, care for his health, his physical, emotional, intellectual and moral development, the protection of the child, maintaining personal contact with the child, ensuring his upbringing and education, determining the place of his residence, representing him and administering his assets and liabilities; it is created upon the child's birth and extinguished upon the child acquiring full legal capacity. The duration and extent of parental responsibility may only be changed by a court.[75]

This regulation is followed by Art. 875, which implements the international legal obligations of the Czech Republic, and according to which "Parents exercise parental responsibility in the best interests of the child." This provision further provides that

> Before making a decision that affects the interests of the child, parents shall inform the child of everything that is necessary for the child to form his own opinion on a given matter and communicate it to the parents; this does not apply if the child is unable to properly receive the message or form his own opinion or communicate it to his parents. Parents shall pay due attention to the child's opinion and take the child's opinion into account when making a decision.[76]

Finally, also relevant is the provision of Art. 876, "Parents exercise parental responsibility in mutual accord."

75 Art. 858 of the Civil Code.
76 Art. 875 of the Civil Code.

The following principles can be deduced from the above regulation. First, parents can make decisions about the child, so they have the right to decide to share a photo, video, quote, etc. Secondly, this right is limited. Parents are limited by the best interests of the child. I confess that I cannot imagine a situation where sharing any information about a child would be in the child's best interest. However, I accept that there may be situations where the impact of such disclosure on a child would be neutral and where it would therefore not be directly contrary to the child's best interests.

Thirdly, there should be a consensus between the parents that photographs or other material relating to the child will be disclosed. And fourth, parents should consider the child's views and not disclose matters without the child's knowledge or against the child's express consent. Here, of course, the problem arises with the maturity of the child, and the ability to evaluate the situation and assess the possible consequences.

Under Czech law, a person acquires legal capacity gradually, in full extent by becoming an adult. Alternatively, in my opinion, Act No. 110/2019 Coll. Act on personal data processing may be considered and applied by analogy. This act provides in Art. 7 that "a child shall enjoy capacity to grant consent to personal data processing in relation to an offer of information society services addressed directly to the child from fifteen years of age." Therefore, I consider the age of 15 years to be a clear threshold in a broader sense, when parents should not disclose anything that may interfere with their child's privacy without the child's consent. In practice, however, parents should also respect the will of the younger child. In fact, the legislation gives the child the opportunity to defend himself against interference with his privacy (and personality) against anyone, including parents exercising parental responsibility.

## 11. Privacy, digital technologies, and Czech labor law

The issue of the use of digital technologies and privacy protection is also very topical in the field of employment law. The interest of employers in using modern technology to monitor the workplace, and consequently the employee, is understandable. Equally understandable is the desire to monitor an employee's work activities and how he or she uses the resources entrusted to him or her, and whether he or she works during normal work hours. The reasons are many, ranging from protecting the employer's property, ensuring the safety of the employee (typically in hazardous locations such as gas stations), preventing the employee from misusing the employer's property for personal use, but also the interest in the efficiency of the employee's work. Against these interests, which are undoubtedly worthy of protection, stand the interests of the employee and his fundamental rights.

The protection of the employer's property interests and the protection of the employee against unwarranted interference with his or her privacy is ensured by 1) the civil law mechanisms described earlier in this chapter; 2) the regulation in the Labor

Code; and 3) based on the GDPR. For practical reasons, it is the protection through the GDPR that is most often used in employment law practice. It is useful, convenient, and cost-free for employees, as enforcement is delegated to an external state authority.

The legal regulation in the Labor Code generally does not allow employers to interfere in the privacy of employees. However, there is an exception to this general rule. The Regulation is contained in Art. 316 of the Czech Labor Code which states:

> Without a serious cause consisting in the employer's nature of activity, the employer may not encroach upon employees' privacy at workplaces and in the employer's common premises by open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee. (3) Where there is a serious cause on the employer's side consisting in the nature of his activity which justifies the introduction of surveillance (monitoring) under subsection (2), the employer shall directly inform the employees of the scope and methods of its implementation.[77]

The purpose of this amendment is summarized in the explanatory memorandum to the Labor Code. It makes it easier to deal with individual situations, since the previous regulation, which was based on the general constitutional principles arising from the Charter of Fundamental Rights and Freedoms and the application of Art. 7(2) of the previous Labor Code on the principle of good morals, was not satisfactory.[78]

As a rule, employees may not use the means of work entrusted to them by their employer for personal use. This rule also applies to computers, phones, tablets, software, etc., regardless of whether such use is to occur during or after working hours.[79] The employer is therefore allowed to check whether the employee complies with this obligation. However, the tools of control are limited by law.

In particular, the legislation in Art. 316(2) of the Labor Code significantly limits the possibility of control by open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee. According to this provision, on the other hand, it does not matter if an employee is monitored by an online camera that is primarily intended for another purpose and the employer only checks the employee *ad hoc*.[80]

First, under Czech law, the employee must be properly informed that he or she will be monitored by the employer. This information must be provided by the employer to each employee individually and conclusively in his or her own interest. The information should be

77 Art. 316 of Czech Labor Code.
78 See explanatory memorandum.
79 This is, by the way, a common problem in academic practice, as faculty members often use the computer and access to professional databases for private law business or court work.
80 Morávek, 2017, p. 948.

> accurate and complete, and must include a statement of the locations at which the monitoring is carried out, the extent and duration of the monitoring, the technical means by which the monitoring is carried out, whether the data collected, e.g., in electronic form, is retained by the employer, for how long it is retained and for what reason it must be retained.[81]

The obligation to inform is by nature reduced in the case of covert control. However, even in this case, the employer must comply with the information obligation in full immediately, but only after it has been completed; in general terms, the employer must declare the possible control at least in advance.[82]

There must be an *objective and compelling reason* for the monitoring, and it must be carried out in a *proportionate* manner[83] and only in certain places (locker rooms or toilets are strictly excluded, even though these places can be very effectively abused by employees to avoid performing their duties). Monitoring will be excluded whenever the objective of the monitoring can be achieved by other means. Less legally problematic is the situation where the employee is only monitored, and no record would be made. In practice, an employer may incorrectly assess the existence of a reason for interfering with employees' rights. For example, in the case of the State Printing Office (*Státní tiskárna cenin*), which monitored employees extensively, such a reason may indeed exist, but this will be true in the case of printing money, but no longer in a situation where the surveillance was done without the employees' consent and when "only" meal and ticket vouchers were printed.[84]

The possibility of controlling electronic mail is problematic, as there is a risk of violating the confidentiality of letters. Nevertheless, the Art. 316(1) of the Labor Code states that:

> Without their employer's consent, employees may not use the employer's means of production and other means necessary for performance of work, including computers and telecommunication technology for their personal needs. The employer is authorized to check compliance with the prohibition laid down in the first sentence in an appropriate way.[85]

81 Morávek, 2014, p. 953.

82 Ibid.

83 According to the Supreme Court: "The court shall consider, in particular, whether the inspection was continuous or subsequent, its duration, scope, whether it restricted the employee's activities at all and to what extent, whether it also interfered with the employee's right to privacy, etc." 21 Cdo 1771/2011.

84 See case of the Municipal Court in Prague 6 Ca 227/2008 analyzed in Veselý, 2017 Jaké jsou možnosti zaměstnavatele při kontrole zaměstnanců a jak je to s instalací kamer se záznamem? [Online] Available at: https://www.epravo.cz/top/clanky/jake-jsou-moznosti-zamestnavatele-pri-kontrole-zamestnancu-a-jak-je-to-s-instalaci-kamer-se-zaznamem-106015.html?mail (Accessed: 22 June 2022).

85 Art. 316, para. 1 of the Czech Labor Code.

Therefore, an employer may check the inbox and electronic mails, but must do so in a reasonable and proportionate manner. Thus, it is necessary to sensitively assess e-mail after e-mail and evaluate in general whether the individual interference with the employee's rights is necessary. This condition will be fulfilled within the scope of the Czech law if the employee is ill for an extended period, the employment relationship has ended, etc. At the same time, control is possible if the identifying features of the message (sender, subject, address) show that it concerns the employer's activities and is not of a private nature. In general, it is easier to access an e-mail box if the e-mail address is a general e-mail address assigned by the employer to the employee and therefore does not contain the employee's personal identification data.

COVID-19 has greatly expanded the possibilities of working outside the workplace, typically from home. In doing so, the employee is using the resources assigned to the job by the employer and should perform the work at the given time. I believe that in such a situation, the employer cannot exercise control any more than it could in a case where the employee is on-site (*in situ*). The rules described above therefore apply in the same way. I further consider that an employer may order an employee to have a camera on in the case of, for example, work meetings conducted online. However, it cannot prohibit the use of technologies that protect the privacy of the employee and his family, such as blurring the image behind the employee. Finally, I believe that an employer cannot force an employee to agree to record a meeting unless there is a compelling reason to do so.

The possibility of performance of work by electronic means has also led to the fact that the work activities of employees are broadcasted online by electronic means even where it did not happen before, for example in teaching, where teachers must lecture in situ plus accept the fact that their performance is broadcasted online. In addition to that, their work is recorded and published online. I believe that the rules contained in Art. 316 of the Labor Code do not, in principle, prevent the employer from ordering such transmission and recording. It is not related to the employee's control, but to the performance of his or her work, which is public by nature.[86]

Employees often tend to resolve any problems through public law by complaining to the State Labor Inspectorate *(Státní úřad inspekce práce*) or the Office for Personal

86 However, different conclusions can be drawn from the ECtHR's decision in *Antović and Mirković v. Montenegro* (Application no. 70838/13). This is indicated by the fact that the opinion I have referred to is supported by the dissenting opinion of Judges Spano, Bianko and Kjolbro, whereas the decision itself does not contain such reasoning and this concept. Those judges in their dissenting opinion state "We emphasize that the applicants are university teachers who were giving lectures in a university amphitheater, thus fully engaged in a professional activity in a quasi-public setting, and not, for example, in their offices. Having been notified of the video surveillance in the amphitheaters, their reasonable expectation of privacy in that particular context, if any, was very limited. In conclusion, the mere fact of the amphitheaters being monitored cannot in our view engage Art. 8 §1 of the Convention without further elements being demonstrated, as we have explained above. By expanding the scope of Art. 8 §1 to include the facts of the present case, the majority have overly broadened the notion of "private life" under that provision, to an extent which lacks a basis in the Court's case law and is not sufficiently supported by cogent legal arguments."

Data Protection (*Úřad pro ochranu osobních údajů*). Nevertheless, their decisions may be and often are reviewed in court proceedings.

Motivation for employers to violate employees' rights often vary. An example of a situation where an employer has interfered with the rights of employees in an effort to primarily protect his property located in his stores, both from employees and from theft by the public, was a case decided by the Municipal Court in Prague known in the Czech Republic as JRC Czech, a.s.[87] In that case, the court held that

> employees have a right to a certain degree of privacy even in the workplace, even if it is by the nature of the employment relationship, is less than, for example, in the employee's own living quarters, since private life and working life cannot be completely separated; a certain private sphere is constantly worn by the with him and the intrusion into it is, in the case of an employee monitored by CCTV significant in that he is monitored continuously throughout all or most of his working hours every day for the majority of the working day.[88]

The court also stated that the possibility of monitoring of employees in the workplace is not strictly prohibited as the Labor Code allows it under certain circumstances. Nevertheless, according to the court,

> The provisions of the Labor Code must be interpreted in accordance with Section 5(2) of the Data Protection Act, which implies that in addition to a compelling reason based on the special nature of the employer's activities, the interest in protecting the employer's rights or legitimate interests outweighs the interest in protecting the private and personal life of employees.[89]

In this case, however, the conditions for monitoring were not met because the monitoring system was set up inappropriately. The employees were monitored, albeit admittedly (i.e., not covertly), but virtually throughout their working time and at high resolution. As the focus of the system was not on the protection of assets, as declared, but on the monitoring of employees, the employer failed in the test of proportionality.[90]

87 8A 182/2010-69-77.

88 This approach is also supported by the case law of the Constitutional Court, which in turn is based on the case law of the ECtHR, see for example decision of the Constitutional Court Pl. ÚS 3/09.

89 Czech Data Protection Act was replaced by GDPR.

90 The court in this case cited previous decision of the Supreme Administrative Court 5 As 158/2012-4 according to which "installation of CCTV cameras systems, taking into account their nature and the interference with the personal integrity of persons, is only possible when all less invasive means have already failed or would not be able to meet the purpose pursued. There is no doubt that a CCTV system, in comparison with other means (e.g., personnel, mechanical) that can achieve the fulfillment of the purposes pursued by the applicant, interferes with fundamental human rights, namely the right to privacy and to private family life […], and therefore to the human dignity from which those rights derive."

Another case concerned the Czech Post, which massively controlled its employees via GPS locators and as a result 7,770 delivery agents were equipped with trackers.[91] The motivation here was different. The employer defended the tracking for several reasons: 1) to speed up and improve the quality of service and facilitate complaints; 2) to optimize the workload of employees; 3) to monitor the movement and load of vehicles; and 4) to ensure the greatest possible safety of employees at work.

In its decision, the Office for Personal Data Protection did not accept these arguments and stated that this type of monitoring of an employee is unlawful. However, the Office for Personal Data Protection's decision also shows that part of the employer's intention was lawful after all. This was because the aim was also to ensure the benefit of its employees and the persons to whom it provides its services, i.e., to optimize delivery districts in terms of employee workload and complaint handling. The sanction imposed was therefore low — only CZK 80,000.

The decision of the Office for Personal Data Protection has also been reviewed by the courts. The Municipal Court upheld the decision of the Office for Personal Data Protection.[92] In doing so, it considered whether the monitoring of the employees was appropriate, necessary, and proportionate. It found that none of these conditions were met. As regards appropriateness, the technology used could not have prevented the delivery agent from failing to deliver the parcel. The criterion of necessity was also not satisfied since it was sufficient to consider whether the delivery driver approached the delivery point (i.e., the addressee of the parcel). The last criterion, proportionality, was judged not to have been met because of the disproportionate interference with the privacy of the delivery persons (every single movement of the delivery agents was monitored).[93]

On the contrary, the Labor Code does not respond to situations where an employee is recorded, photographed, or monitored by a third party. This could be, for example, a citizen attending a meeting of a public administration body or filming a police officer[94] during an intervention, or a politician in the context of his political activities. A third party can also be a student who films a teacher's online lecture. Undoubtedly, the employer has a duty of prevention in which it should limit the possible risks associated with the performance of the employee's work activity and his right to privacy, if possible. For example, the lecture can be transmitted online under authenticated access and not in full public view, etc.

91 Decision of the Office for Personal Data Protection No. UOOU-00237/13-38.

92 Decision of the Municipal Court in Prague No. 6A 42/2013 5.

93 Bednář and Metelka, 2017, *GPS monitoring zaměstnanců podruhé* [Online] Available at: https://www.epravo.cz/top/clanky/gps-monitoring-zamestnancu-podruhe-106141.html (Accessed: 22 June 2022).

94 Opinion of the Security Policy Department of the Ministry of the Interior on the recording of police officers while on duty.

## 12. Right to privacy and digital evidence in criminal law

In the field of criminal law, the issue of digital technology and privacy law is particularly relevant in evidence at criminal investigation and trial.[95] According to Art. 89(2) of the Code of Criminal Procedure, evidence can be anything, including audio or visual recordings.[96] The advantage of such evidence is that it is able to provide a range of data and reliably prove a particular fact.[97] It would therefore be a pity not to take advantage of the possibilities offered by modern technology. From a privacy perspective, situations where recordings are made without the knowledge of the person being recorded are problematic. However, it is precisely such recordings that can be of the highest probative value and can also be the only direct evidence. Three key questions have emerged: 1) what procedural conditions must be met for covert surveillance and recording to be possible? 2) Can a privately made recording also be used as evidence? 3) Can evidence obtained by covert recording in one proceeding also be used in another proceeding?

As regards procedural conditions, they are set out in Art. 158d of the Code of Criminal Procedure which regulates the *Surveillance of Persons and Items as follows:*

> (1) Surveillance of persons and items (hereinafter referred to as "surveillance") shall be understood as acquiring knowledge on persons and items conducted in a classified manner by technical or other means. If a Police authority ascertains that the accused person is communicating with his defense counsel, it is obliged to destroy the record containing this communication and not to use facts learned in this connection in any way. (2) Surveillance, during which any audio, visual or other records shall be made, may be performed solely based on written authorization of a public prosecutor. (3) If the surveillance should interfere with the inviolability of residence, inviolability of letters or if it should investigate the contents of other documents and records kept in privacy by use of technical means, it can be performed solely based on prior authorization of a judge. When entering residences, only steps related to the placement of technical devices may be made. (4) Authorization according to sub-sections (2) and (3) may be issued only upon a written request. The request must be reasoned by a suspicion of a specific criminal activity and if known, also by data on persons or items that are to be monitored. The authorization shall state a time limit, for which the surveillance shall be conducted and that cannot exceed six months. The authority that authorized the surveillance may prolong the time limit by a written order issued based on a new written request, always for a time limit not exceeding six months. (5) If the matter cannot be delayed and if cases referred to in sub-section (3) are not

95 The technical aspects of digital evidence are comprehensively described and analyzed in publication Polčák et al., 2015.

96 Art. 89, para. 2 of the Code of Criminal Procedure stipulates: "Evidence may be anything that can help to clarify the case."

97 Deepfake technology relativizes this claim.

> concerned, the surveillance may be initiated even without authorization. However, the Police authority is obliged to immediately request the authorization, and if it is not granted within 48 hours, it is obliged to terminate the surveillance, destroy any eventual records and not use information so ascertained in any way. (6) Without fulfilling the conditions according to sub-sections (2) and (3) may the surveillance be conducted if the person, whose rights and liberties are to be interfered with, grants his explicit consent therewith. If this consent is post facto withdrawn, the surveillance shall be immediately terminated.[98]

From the above it is evident that the Czech legislation distinguishes between 1) surveillance that *does not interfere with the privacy of the monitored person*. In this case, it is the *prosecutor* who gives consent to the surveillance; and 2) situations where *there is an interference with privacy* and therefore a higher level of protection is required. The latter is ensured by the fact that the permission for surveillance must be given by *a judge*. Without the consent of a prosecutor or a judge, the recording is not admissible and thus cannot be used procedurally.

The Code of Criminal Procedure further responds to the issue of modern technology in a relatively new Art. 7b. According to this provision:

> (1) Where it is necessary to prevent the loss, destruction or alteration of data relevant to criminal proceedings which are stored in a computer system or on a medium, the person who holds or has under his control the data may be ordered to preserve such data in an unaltered form for such period as may be specified in the order and to take such steps as may be necessary to prevent disclosure of the fact that the data have been ordered to be preserved. (2) Where necessary to prevent the continuation or repetition of criminal activity, a person who holds or has under his control data stored in a computer system or on a medium may be ordered to prevent other persons from accessing such data. (3) An order under subsection (1) or (2) may be issued by the president of the chamber and, in pre-trial proceedings, by the public prosecutor or police authority. The police authority shall require the prior consent of the public prosecutor to issue such an order; without prior consent, an order may be issued by the police authority only if prior consent cannot be obtained and the matter cannot be delayed. (4) An order under subsection (1) or (2) shall specify the data to which the order relates, the reason for which the data are to be retained or access to them is to be prevented and the period for which the data are to be retained or prevented, which shall not exceed 90 days. The order shall include a statement of the consequences of non-compliance. (5) The authority which has issued an order under subsection (1) or (2) shall promptly deliver it to the person against whom it is directed.

This provision responds to the problem of the ephemeral nature of electronic data. However, there is still no consensus in current practice on how to apply this

98 Art. 158d of the Code of Criminal Procedure.

provision in relation to the provisions of Art. 158d of the Code of Criminal Procedure. A request for data to be "frozen" typically precedes a court's decision that the surveillance may be conducted. Once such a decision is made, however, the police seek the release of the data from the time they receive their request. In practice, this means that the police also request the data that preceded the court's decision. From this perspective, the court's decision could have a retroactive effect, which some attorneys question because of its conflict Art. 158d with the Code of Criminal Procedure.[99]

Interception and recording of telecommunications traffic is carried out based on Art. 88 of the Criminal Procedure Code. In principle, the president of the Senate is authorized to order the interception and recording of telecommunications traffic and, in pre-trial proceedings, judge on the motion of the public prosecutor. They may do so only in specified cases and only in compliance with the principle of proportionality. The possibility of interception and recording of telecommunications traffic in a situation where the accused is communicating with his defense counsel is wholly excluded.

The practical issue is the possibility of using evidence obtained legally in one case to prove another case. Interception and recording of telecommunication traffic carried out based on Art. 88 of the Criminal Procedure Code can, in principle, be used in another case. A recording made during surveillance pursuant to Art. 158d (2) of the Criminal Procedure Code may also be used in another case. For the same conclusion in relation to Art. 158d para. 3, which concerns intrusions into an individual's privacy, a similar permission is missing in the law. This fact limits the possibility of using spatial interceptions as evidence in other criminal proceedings.

## 13. Private recordings as evidence in criminal and administrative proceedings

The procedural rules allowing surveillance, by which the law restricts the State and its organs, do not naturally apply to individuals — private persons. Nevertheless, the use of a private recording as evidence is not self-evident, as the rights of the person who was recorded must also be respected. The Czech Supreme Court already acknowledged the possibility of using such a recording in 2007 when it stated:

> With regard to the provisions of Art. 89(2) of the Criminal Procedure Code, the possibility of using as evidence a sound recording made by a private person without the consent of the persons whose voice is so recorded cannot in principle be excluded.

99 Odborníkům se nelíbí, že policie žádá o vydání Internetových dat bez souhlasu soudu, 2019, [Online] Available at: https://www.ceska-justice.cz/2019/08/odbornikum-se-nelibi-ze-policie-zada-vydani-Internetovych-dat-bez-souhlasu-soudu/ (Accessed: 07 September 2022).

> Art. 88 of the Code of Criminal Procedure does not apply here, even by analogy. However, the admissibility of such evidence must always be assessed also regarding respect for the right to privacy enshrined in Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and the right to inviolability of the person and his or her privacy within the meaning of Art. 7(1) and Art. 10(2) of the Charter of Fundamental Rights and Freedoms.

In addition, even in the criminal procedure it is relevant whether the facts of the case can also be proved by other/additional evidence.

The Czech courts have addressed the issue of private recording evidence in the following decisions:[100]

Case No. II. ÚS 143/06, in which the Constitutional Court admitted evidence of a covertly made tape recording of a telephone call. It stated:

> The basic criterion which should ultimately lead to a decision on the applicability or inapplicability of the information thus obtained as evidence in the relevant proceedings will be the balancing of the protected rights and interests which clash in this private sphere, and where the state becomes the arbiter (usually through the court) deciding on it, which of these interests will prevail in a given specific conflict, while the assessment of the applicability or inapplicability of the information thus obtained (and submitted to the state in one way or another) will be carried out according to procedural norms, which, however, only define the rules for how to properly determine the facts and find the "substantive" law, i.e., to decide on the actual subject of the dispute. Therefore, in addition to the circumstances in which such a recording was made, the relevance of the interest at stake in the proceedings themselves and the options available to the party claiming that information to obtain that information by means other than at the cost of violating the other person's privacy will be decisive for the final assessment of the case.

Case No. IV. ÚS 2425/09. Here, the Constitutional Court concluded that

> In assessing the objection of violation of the right to privacy by the taking of the said recording, the complainant can be accepted that the monitoring of a public place by a camera and the subsequent taking of a permanent recording fall under the protection provided by Art. 10 of the Charter and Art. 8(8)(a) of the Constitution. In general, to assess whether there has been an unlawful interference with privacy by public authorities, it is necessary to examine whether a private matter or a public event was recorded and whether the material obtained was intended for limited use or was intended to be available to the public…The routine use of security cameras, whether on the street or on premises such as a shopping center or police station, where they

100 The case law of the Czech courts was well mapped in Zaoralová's article (Zaoralová, 2017, pp. 28–32.).

> serve a legitimate and foreseeable purpose, is not in itself problematic in the light of Art. 8 §1 of the Convention…The above conclusions are fully applicable to the complainant's case, since the victim, by installing an industrial camera in a public place, pursued a legitimate aim, i.e., the protection of his property and the detection of the perpetrator of a crime that would affect him personally. The footage was then used only for a strictly necessary purpose (proving the complainant's guilt in criminal proceedings) and was not abused in any way, e.g., by making the footage publicly available, by disparaging the complainant in the media, etc. Therefore, it can be concluded that the installation of the industrial camera and the footage obtained by it does not fulfill the characteristics of a violation of the complainant's constitutionally guaranteed right to protection of privacy.

In contrast to the previous decision concerning monitoring a public place, in the Supreme Court's decision No. 3 Tdo 803/2009, audio and video recordings from a private mobile phone were used as evidence and found admissible.

In a recent decision 3 Tdo 925/2020, the Supreme Court further confirmed and clarified the conditions for the use of a recording made by a private person. The court stated:

> As regards the audio recording made by the victim, nothing prevented its admission as evidence in the case (cf. Supreme Court Resolution of 3 May 2007, Case No. 5 Tdo 459/2007…). Moreover, it was only supporting evidence, while the conclusion of the accused person's guilt was based on the other evidence already mentioned. In the present case, the presence of so-called omitted evidence cannot be found either, since the courts did not omit the defendant's motions for supplementing the evidence, duly dealt with them, and explained why it had rejected them for redundancy.

Another important conclusion follows from the above—in criminal proceedings, evidence that a private person produces himself and that can be used against himself may also be applicable. This may be, for example, a recording from a dashboard camera in a car, from a phone or a smartwatch, i.e., common electronics that we wear and use primarily to help us.

The use of evidence of a recording of a person's image that interferes with that person's personality rights in *administrative proceedings* is based on similar principles to those underlying such use in criminal proceedings. In administrative proceedings, too, there is therefore a distinction depending on who made the recording, whether it was another private person or a public authority. If the recording was made by a public authority, it is applicable only if the law expressly so provides and in addition to that all the conditions required by law must be strictly complied with. In the case of a private person, on the other hand, it may be the case that the statutory conditions are not met (e.g., the qualified consent provided for in the Civil Code is missing or the conditions set out in the GDPR are not fulfilled), but the recording evidence will nevertheless be admissible. According to Supreme Administrative Court, in case

of non-compliance with the law, the administrative court must apply the proportionality test. This test assesses the legitimacy of the objective sought to be achieved by the recording and the proportionality of the procedure used. It is assessed whether, in a particular case, the protection of the personality rights of the subject concerned may outweigh the interest of society in clarifying and punishing the offences and, above all, the protection of the constitutionally guaranteed rights of the maker of the recording.[101]

## 14. Privacy and COVID-19 — Concluding remarks

Partly outside the substantive framework and focus of the whole chapter is the issue of the measures taken by the Czech Republic during the COVID-19 disease pandemic. The focus of the legislation that applies to this issue lies primarily in the area regulated by the GDPR, which I did not intent to deal with. However, it is a topical issue that relates both to the effective use of modern technology and the protection of privacy. At the same time, the reaction of the Czech State reveals some structural issues that are unfortunately typical of the public administration of the Czech Republic. I will therefore, briefly discuss this issue as well.

In response to COVID-19, the Czech Republic introduced several anti-epidemic measures based on the use of digital technologies. The Tečka and čTečka apps were introduced, and both processed the personal data of individuals. These applications were used to prove and check that a person had been vaccinated or had a valid negative test, or had already had a COVID-19 infection.

But the crux of the problem was that the Czech Republic was unable to adopt a satisfactory and functional legal framework. The Office for Personal Data Protection has criticized this situation. This office has repeatedly called for establishing a clear and permanent framework for the processing of personal data. This office has further criticized that the existing legislation is too general and does not contain any system of graduated legal limits. As a result, the Czech administrative courts repeatedly annulled administrative measures by which the Czech government addressed the problem. At the same time, it would be correct and appropriate for the State to regulate the issue by law instead of administrative measures.

From the point of view of the protection of privacy, it is significant that the Czech sate has made it possible to delegate to private persons the performance of activities carried out in the framework of an epidemiological investigation, which consists of the discovery of information relevant the epidemiological situation. The legal basis

101 2 As 45/2010–68.

for such a transfer is a public contract.[102] The fight against COVID-19 also included tracing the population and the legal regulation of their isolation or quarantine. Notifications of the order for isolation or quarantine were sent orally or in writing by the public health authorities, including by telecommunication. The problem, however, was that the Czech Republic failed to digitize the actual tracing of infected residents. Only the eRouška application was introduced, which theoretically worked on the principle of estimating the probability of infection based on the distance from the contact with the infected person and the duration of the contact. This app could not be described as genuinely functional in practice. The authorities, therefore, routed the contacts of the infected person classically by telephone, and as the pandemic progressed, the system became overwhelmed and essentially stopped working altogether. The state only managed meaningful use of modern digital technologies in relation to crossing state borders as the state used the services of mobile operators to send informational text messages.

It is difficult to assess what was behind the failure of the Czech state to make better use of digital technology to protect public health. Whether it was doubts about how to set up the system so that it did not conflict with the right to privacy, or whether it was a failure to adopt general legislation that would provide the necessary legal basis for the introduction of technical solutions. However, it seems to me that the right to privacy is sometimes used in the Czech Republic as one of those easy and cheap explanations for why some things fail to be implemented by the Czech public administration. COVID-19 and the reactions to it demonstrate this well.

102 Art. 62a of Act No. 258/2000 Coll., the Act on the Protection of Public Health and on Amendments to Certain Related Acts.

# Bibliography


Bednář, S., Metelka, J. (2017) *GPS monitoring zaměstnanců podruhé* [Online]. Available at: https://www.epravo.cz/top/clanky/gps-monitoring-zamestnancu-podruhe-106141.html (Accessed: 22 June 2022).

Bónová, K. (2022) 'Ochrana soukromí ve veřejném prostoru', *Revue pro právo a technologie*, 13(25), pp. 157–225 [Online]. Available at: https://doi.org/10.5817/RPT2022-1-4 (Accessed: 22 October 2022).

Dvořák, T. (2014) '§ 135 Ochrana názvu, pověsti a soukromí' in Švestka, J., Dvořák, J., Fiala, J., Pelikánová, I., Pelikán, R., Dvořák, T., Svoboda, K., Pavlík, P. (eds.) *Občanský zákoník – Komentář – Svazek I (obecná část)*. Praha: Wolters Kluwer, pp. 464–471.

Filip, J. (2011) 'Úvodní poznámky k problematice práva na soukromí' in Šimíček, V. (ed.) *Právo na soukromí*. Brno: Masarykova univerzita, Muni PRESS, pp. 9–19.

Nechvátalová, L. (2021) 'Čl. 7 Právo na respektování tělesné a duševní integrity osoby a zákaz mučení a špatného zacházení' in Husseini, F., Bartoň, M., Kokeš, M., Kopa, M. (eds.) *Listina základních práv a svobod. Komentář.* 1st edn. Praha: C. H. Beck. pp. 224–245.

Kočí, P. (2011) *Případ šmírujícího MacBooku – co v Televizních novinách nebylo* [Online]. Available at: https://www.lupa.cz/clanky/pripad-smirujiciho-macbooku-co-v-televiznich-novinach-nebylo/ (Accessed: 22 June 2022).

Kokeš, M. (2012) 'Čl. 12 Soukromí v prostorové dimenzi' in Wagnerová, E. (ed.) *Listina základních práv a svobod: Komentář.* Praha: Wolters Kluwer, pp. 330–340.

Langášek, T. (2012) 'Čl. 7 Nedotknutelnost osoby a zákaz mučení' in Wagnerová, E. (ed.) *Listina základních práv a svobod: Komentář.* Praha: Wolters Kluwer, pp. 186–216.

Lasák, J. (2014) '§ 713 [Ochrana názvu, pověsti a soukromí]' in Lavický, P. (ed.) *Občanský zákoník I Obecná část (§ 1 – 654)*. Praha: C. H. Beck. pp. 711–721.

Míšek, J. (2020) *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita.

Míšek, J. (2017) 'Is the Definition of Personal Data Flawed? Hyperlink as Personal Data (Processing)', in Svantesson, D. J. B., Kloza, D. (eds.) *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*. Cambridge: Intersentia, pp. 331–346; https://doi.org/10.1017/9781780685786.019.

Míšek, J., Kasl, F., Loutocký, P. (2020) 'Czech Republic: Personal Data Protection Law', *European Data Protection Law Review*, 2(6) pp. 289–293 [Online]. Available at: https://doi.org/10.21552/edpl/2020/2/15 (Accessed: 22 October 2022).

Míšek, J., Bartoš, V. (2020) 'Nesnesitelná lehkost zpracování osobních údajů orgány veřejné správy', *Revue pro právo a technologie*, 11(22), pp. 145–174 [Online]. Available at: https://doi.org/10.5817/RPT2020-2-5 (Accessed: 22 October 2022).

Míšek, J. (2014a) 'Consent to personal data processing – The panacea or the dead end?', *Masaryk University Journal of Law and Technology*, 8(1), pp. 69–83.

Míšek, J. (2014b) 'Souhlas se zpracováním osobních údajů za časů Internetu' *Revue pro právo a technologie*', 5(9), pp. 3–74.

Míšek, J. (2014c) 'Vyhledávač jako správce osobních údajů', *Revue pro právo a technologie*, 5(9), pp. 227–229.

Molek, P. (2017) *Základní práva. Svazek první – Důstojnost*. Praha: Wolters Kluwer.

Morávek, J. (2017) '§ 316 Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance' in Pichrt, J. (ed.) *Zákoník práce: Zákon o kolektivním vyjednávání*, Praktický komentář. Praha: Wolters Kluwer, pp. 943–958.

Nonneman, F. (2012) 'Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů', *Právní rozhledy*, 2012/13–14, pp. 505–509.

Ondřejová, E. (2016) *Ochrana osobnosti v common law a českém právu*. Praha: Leges.

Pavlík, P. (2014) '§ 84 Podoba člověka' in Švestka, J., Dvořák, J., Fiala, J., Pelikánová, I., Pelikán, R., Dvořák, T., Svoboda, K., Pavlík, P. (eds.) *Občanský zákoník – Komentář – Svazek I (obecná část)*. Praha: Wolters Kluwer, pp. 321–325.

Pelikán, R., Pelikánová, I. (2014) '§ 3 Zásady soukromého práva' in Švestka, J., Dvořák, J., Fiala, J., Pelikánová, I., Pelikán, R., Dvořák, T., Svoboda, K., Pavlík, P. (eds.) *Občanský zákoník – Komentář – Svazek I (obecná část)*. Praha: Wolters Kluwer, pp. 20–30.

Polčák, R., Púry, F., Harašta, J. (2015) *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita.

Pokorný, M. (2017) *Šmírovaní uživatelé kradeného notebooku si na odškodné počkají. Soud musí případ znovu projednat* [Online]. Available at: https://zpravy.aktualne.cz/domaci/smirovani-uzivatele-kradeneho-notebooku-si-na-odskodne-pocka/r~874defd01f6211e7bc5500259060 4f2e/ (Accessed: 22 June 2022).

Solove, D.J. (2011) *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven: Yale University Press.

Veselý, P. (2017) *Jaké jsou možnosti zaměstnavatele při kontrole zaměstnanců a jak je to s instalací kamer se záznamem?* [Online]. Available at: https://www.epravo.cz/top/clanky/jake-jsou-moznosti-zamestnavatele-pri-kontrole-zamestnancu-a-jak-je-to-s-instalaci-kamer-se-zaznamem-106015.html?mail (Accessed: 22 June 2022).

Wagnerová, E. (2012) 'Čl. 10 Právo na soukromí v širším smyslu' in Pospíšil, I., Langášek, T., Šimíček, V., Wagnerová, E. (eds.) *Listina základních práv a svobod: Komentář*. Praha: Wolters Kluwer, pp. 277–299.

Zaoralová, P. (2017) 'Použitelnost soukromých zvukových a obrazových záznamů jako důkazu v trestním řízení', *Bulletin Advokacie*, 2017/11, pp. 29–34.

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.

Chapter IX

# The Right to Privacy in the Digital Age: A Perspective from the Republic of Poland

Bartłomiej Oręziak

## 1. Introduction

This study will analyze the right to privacy in the digital age from the perspective of the Polish normative system with general theoretical elements. The main axis of this perspective is national in nature,[1] as it should be assessed from the point of view of the Polish legal system. It appears that it may have its specificity resulting from local civilization, cultural, social or economic conditions.[2] It seems reasonable to say that just like most modern countries are characterized by differences, their legal systems are also different. These differences are sometimes greater and sometimes smaller, but they usually occur, because they also result from different concepts of law that underlie a particular statehood.[3] The way the right to privacy is analyzed from the general theoretical perspective or from the international human rights law perspective is different. In the first case, the considerations are theoretical and mostly relate to a selected problem common to the

1 Some other sample studies containing a country analysis include: Holtz-Bacha, 2004, pp. 41–52; Trouille, 2000, pp. 199–208; Barnett, 1999, pp. 555–581; Antoš, 2019, pp. 47–55.

2 For example, such elements are highlighted by the European Court of Human Rights in its doctrine of the margin of appreciation (see Arai, 1998, pp. 41–61).

3 Perhaps one of the best-known examples is comparison between the concepts of continental and the Anglo-Saxon law (see Graff, 2008, pp. 60–83; Wiel, 1918, pp. 245–267).

Bartłomiej Oręziak (2023) The Right to Privacy in the Digital Age: A Perspective from the Republic of Poland. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 311–343. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_9

generally understood right to privacy.[4] In the second case, we usually deal with analyzes that are universal or regional in nature.[5] In the universal aspect, the scope of the right to privacy is understood globally and, in principle, the same for everyone. In the second case, there are differences, but they are of a completely different type from those from the national perspective, because they, as a rule, concern the differences that occur on selected continents of the world. However, it is important to bear in mind the situations in which one geographic continent has more than one regional system of human rights protection. This is the case in Europe where, for example, both the legal regime of the Council of Europe operates[6] as well as one of the European Union.[7] In both these cases, the right to privacy is broadly and effectively protected and guaranteed. Nevertheless, there are also differences here, although they are much smaller than in the case of comparing, for example, the European standard of the right to privacy with the American standard.[8] This study aims to present the Polish approach to the right to privacy with general theoretical elements based on several main analytical segments. First, considerations about digital reality as a new space for the right to privacy will be highlighted. Second, an attempt will be made to define the right to privacy. Third, the right to privacy will be presented in the light of constitutional regulations. Fourth, the right to privacy in civil law will be presented. Fifth, the right to privacy in criminal law and trial will be presented. Sixth, the right to privacy in administrative law will be discussed. Each of these elements will be analyzed not only from the point of view of the traditional legal sciences, but also from the point of view of the digital age, where the application of modern technologies for practical use is not without significance for the right to privacy. The study will conclude with a concise summary.

4 See Thomson, 1975, pp. 737–807; McCloskey, 1980, pp. 17–38; Marmor, 2015, pp. 3–26; O'Brien, 1902, pp. 437–448; Diggelmann and Cleis, 2014, pp. 441–458; Weinreb, 2000, pp. 25–44; Speed, 1896, pp. 64–74; Alfino and Mayes, 2003, pp. 1–18; McKay, 1965, pp. 259–282; Van Den Haag, 2017, pp. 149–168; Zaleski, 1998, pp. 218–238; Michałowska, 2013, pp. 51–64.

5 See Madsen, 1992, pp. 231–1012; Hijmans, 2016, cited in Hijmans, pp. 17–75; van der Sloot, 2017, cited in Taylor, Floridi and van der Sloot, 2017, pp. 197–224.

6 Milanović and Papić, 2018, pp. 779–800; McGregor, 2015, pp. 607–634.

7 Nakanishi, 2018, pp. 3–21; Korenica, 2015, pp. 35–70.

8 According to Art. 11 American Convention on Human Rights of November 22, 1969, "1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks." (Zubik, 2008, pp. 99–112).

## 2. Digital reality as a new space for the right to privacy

First of all, it is necessary to answer the question about the features of digital reality. Digital reality is nothing more than some new, nonmaterial space of human activity built with the use of new technologies. It seems that a good term to describe this phenomenon quite precisely is the concept of the cyberspace.[9] In Poland, this term has a legal definition. Pursuant to Art. 2 clause 1 of the Act of 29 August 2002 on Martial Law and the Competences of the Commander-in-Chief of the Armed Forces and the Rules of his Subordination to the Constitutional Authorities of the Republic of Poland**,** which, while implementing the issue of cybersecurity into the Polish normative system, at the same time introduced a legal definition of cyberspace:

> Cyberspace, referred to in paragraph 1, shall mean the space for the processing and exchange of information created by information and communication systems referred to in Art. 3 point 3 of the Act of February 17, 2005 in the Computerization of the Operations of Entities Performing Public Tasks (Journal of Laws of 2017, item 570), including the links between them and relations with the users.[10]

As the content of this definition shows, to fully decode the meaning of cyberspace in Poland, it is necessary to refer to the legal definition of IT systems. Such definition is Art. 3 point 3 of the Act of February 17, 2005, in the Computerization of the Operations of Entities Performing Public Tasks, according to which the ICT system is

> a set of cooperating IT devices and software, ensuring processing and storage, as well as sending and receiving data through telecommunications networks using a terminal device appropriate for a given type of network within the meaning of the Telecommunications Law of July 16, 2004 (Journal of Laws of 2021, item 576).[11]

Unfortunately, there is another statutory reference to this definition. Thus, in accordance with Art. 2 point 43) of the Act of July 16, 2004—the Telecommunications Law: "Telecommunications terminal equipment is telecommunications equipment intended for connection directly or indirectly to network termination points."[12]

9 Ning et al., 2018, pp. 1843–1856; Zdzikot, 2022, cited in Chałubińska-Jentkiewicz, Radoniewicz and Zieliński, 2021, pp. 9–21.

10 The Act of 29 August 2002 on Martial Law and the Competences of the Commander-in-Chief of the Armed Forces and the Rules of his Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Journal of Laws of 2017, item 1932, of 2022, item 655).

11 The Act of February 17, 2005, on computerization of activities of entities performing public tasks (consolidated text, Journal of Laws of 2021, item 2070).

12 The Act of July 16, 2004, Telecommunications Law (consolidated text, Journal of Laws of 2021, item 576, of 2022, item 501).

To sum up, after decoding the meaning of all statutory references, in accordance with Polish law, cyberspace should be understood as the space of information processing and exchange created by a set of cooperating IT devices and software ensuring processing, storage, as well as sending and receiving data via telecommunications networks using the appropriate for a given type of telecommunications network, a telecommunications device intended to be connected directly or indirectly to network termination points, together with connections between them and relations with the users.[13]

The presented understanding of the concept is, first of all, of a legal nature, secondly, of a technical nature, and thirdly, it does not disregard the fact that cyberspace is a new space for human activity.[14] On the one hand, it was provided for in generally applicable law in Poland. On the other hand, it draws attention to the multi-component nature of cyberspace. We are dealing here with the material (physical) and nonmaterial (not physical) aspect and from this definition we can interpret two specific dimensions of cyberspace. We are talking here about the horizontal and vertical dimension, as the discussed definition not only provides for the functioning of mutual interactions between ICT systems within cyberspace, but also the correlation of the ICT system with the user and users with users as well. Therefore, the Polish definition proposal deserves recognition. The more so as the introduction of a definition of cyberspace to the generally applicable legal system is rare on a global scale.[15] However, it has one notable imperfection. It contains a statutory reference, which results in two subsequent references. It seems to be completely unnecessary. This disrupts the possibility of an easier understanding of generally applicable law, and it certainly does not favor the postulate of legal transparency. We are talking about such important issues as the principle of correct legislation[16] and the principle of specificity of legal provisions.[17] Nevertheless, apart from the observed imperfection, the Polish solution deserves considerable praise.

Returning to the definition of the features of cyberspace as a digital space constituting a new space for the right to privacy, it should be noted that the concept of cyberspace was not created by lawyers for the needs of a specific normative order. The first definition of cyberspace was presented in 1982 by William Gibson, the author of a fantasy novel entitled *Burning Chrome*. It was a world of virtual reality generated by computer programs, provided with images, animations, sound and a wide range of free choice.[18] Two years later, in his next work, *Neuromancer*, he described cyberspace as follows:

13 Ferens, 2021, pp. 31–50; Snopkiewicz, 2020, pp. 29–41.
14 Marczyk, 2018, pp. 59–72; Kaszuba, 2020, pp. 49–72; Băncilă, 2018, pp. 5–10.
15 Oręziak, 2019, pp. 34–39.
16 Działocha and Zalasiński, 2006, pp. 5–6; Wronkowska, 2006, cited in Zubik, 2006, p. 673; Nowacki, 1995, p. 98.
17 Verdict of the Constitutional Tribunal on March 21, 2001, file ref. act K 24/00; Verdict of the Constitutional Tribunal of May 22, 2002, file ref. act K 6/02; Verdict of the Constitutional Tribunal of November 20, 2002, file ref. file K 41/02.
18 Nowak, 2013, p. 6.

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.[19]

Although we are dealing here with a definition contained in a literary work colored with fiction, it cannot be denied that it is pioneering,[20] for determining the direction of thinking. It is worth pointing out that despite the lack of a scientific character, the discussed definition emphasizes the basic properties of cyberspace. It can be interpreted as: a) illusory, an imaginary world that is to some extent based on an illusion; b) voluntary, as participation in cyberspace is based on the consent of its participants; c) globality understood as territorial accessibility to cyberspace, in principle, in every corner of the world; d) universality understood as the universal popularity of cyberspace;[21] e) complexity in the sense of complexity, the enormous amount and multidimensionality of the data posted. The above basic catalog of cyberspace attributes is an example and is an original proposal for the interpretation of the definition created by William Gibson. In the literature, one can find additional proposals for the features attributed to the concept of cyberspace. We are talking about attributes such as: "plasticity, fluidity, computability, accuracy, repeatability, hypertext, interactivity, visuality, compatibility, openness, limitlessness, versatility, complexity, network, acumen, convergence, consolidation, automation and totality."[22]

Therefore, cyberspace is presented as a new intangible space of human activity with its own specific features. What is noticeable here is the desire to reproduce traditional life in the digital world. There are increased possibilities and they are of various nature. From the most basic ones like shopping, communicating with other people, watching movies, listening to music or posting links[23] to the more advanced ones, such as healing yourself (digital medicine,[24] e-health,[25] m-health,[26] telehealth,[27] telemedicine,[28] telecare,[29] sensory health[30]), obtaining electronic evidence,[31] using

19 Gibson, 2009, p. 59; Sienkiewicz, 2009, cited in Jemioła, Kiesielnicki and Rajchel, 2009, p. 194.
20 First known definition of cyberspace.
21 It is estimated that by 2021, 63% of the world's population have used the Internet, see Facts and Figures 2021: 2.9 billion people still offline. https://www.itu.int/hub/2021/11/facts-and-figures-2021-2-9-billion-people-still-offline/.
22 Janowski, 2012, cited in Galewska and Kotecka, 2012, p. 394.
23 Ohly, 2018, pp. 664–675.
24 Elenko, Underwood and Zohar, 2015, pp. 456–461.
25 de Pietro and Francetic, 2018, pp. 69–74.
26 Sezgin, 2018, cited in Sezgin, Yildirim and Sumuer, 2018, p. 1.
27 Wang et al., 2014, pp. 314–324.
28 Linkous, 2001, p. 226.
29 Afsarmanesh, Masís and Hertzberger, 2004, cited in Camarinha-Matos and Afsarmanesh, 2004, pp. 211–212.
30 Gao et al., 2020, cited in Xu et al., 2020, pp. 55–56.
31 Shapiro, 1999, pp. 14–27; Hancock, 2000, pp. 306–307; Wible, 2003, pp. 1577–1623.

new means of payment,[32] and profiling of personal data.[33] In addition to all of this, there is a wider and more common use of artificial intelligence algorithms.[34] The spectrum of designations of modern technologies and the related digital transformation of human life raises many legal problems, such as defining the principles of legal liability [35] or applicable law.[36] In addition, it is worth signaling at this point that the concept of cyberspace is also understood from the psychological and sociological point of view[37] and in this dimension it is defined as "any space where people can gather their minds without taking their bodies there".[38] It is also indicated that this is the new Tower of Babel, a place where world cultures, ideas and information can be shared and disseminated in real time, while exclusion from this digital world condemns people to isolation.[39]

Regardless of how the concept of cyberspace is understood, what features it has, what designates it has and what consequences they have, there is one more very important and fundamentally determining factor in the shape of cyberspace. That factor is a human. Human participation prevents any creation of cyberspace on autonomously defined principles. This means that cyberspace as a creation by a man, as a rule subordinate to it, must be adapted to the currently applicable legal principles. These principles show that a person enjoys certain rights and freedoms, regardless of where they are active. We are talking here about the entire system of human rights protection, where one can only indicate, for example, the freedom of expression[40] or the right to health.[41] Therefore, human brings to cyberspace all the rights and freedoms that belong to him/her because she or he is a human and that have been developed in the traditional world. One of such rights is the right to privacy.[42] This individual entitlement in the digital world should be as widely guaranteed as it is outside cyberspace. Additionally, it seems that it is not about changing the whole concept of the right to privacy, but more about a modern definition of how it is protected. Modern law should provide for a number of effective legal measures adapted to the new conditions of human functioning in cyberspace. It is also important that

32 Miller, 2014, p. 12; Sieroń, 2013, p. 31.
33 Wachter, 2018, pp. 436–449; Mendoza and Bygrave, 2017, pp. 77–98.
34 Jankowska, 2015, cited in Bielska-Brodziak, 2015, pp. 171–197.
35 See Proposal for a Regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final.
36 Świerczyński and Żarnowiec, 2019, pp. 101–135.
37 Tadeusiewicz, 2007, cited in Mastalerz, Pytel and Noga, 2007, p. 23.
38 Dobrzeniecki, 2004, p. 18.
39 Défense et sécurité des systèmes d'information Stratégie de la France. https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.
40 Izyumenko, 2016, pp. 115–130.
41 Piechota, 2012, pp. 93–104.
42 Wójtowicz and Cellary, 2018, pp. 77–96; Rojszczak, 2020, pp. 22–44.

such protection is flexible and constantly updated in line with the ongoing technical, technological, and civilization progress.

Polish law provides for a number of regulations in the field of the right to privacy, ranging from constitutional law through civil law, substantive criminal law, procedural criminal law and administrative law. It is important to present the protection of the right to privacy across the entire system of Polish law. An important question in this regard is also the question of the usefulness and significance of these provisions in the digital reality.

## 3. Attempting to define the right to privacy

Before the analysis presented in this chapter focuses on issues directly related to the Polish legal order, it is necessary to present terminology issues. There are many semantic difficulties in trying to define the right to privacy. It should be noted, however, that this concept is derivative and is essentially determined by the concept of privacy.[43] In the Polish legal literature, many scientific articles can be found on legal measures to protect privacy, privacy as the entitlement of each individual, or the privacy itself. [44] The vast majority of authors present various definitions of terms related thematically to the general sphere of human privacy. Nevertheless, from a methodological point of view, to define, at least approximately, what the right to privacy is, the first step is to answer the question of what privacy is. This is an extremely difficult task as privacy is a highly subjective concept. Each person can understand their privacy individually and have different sensitivity associated with it. In other words, where one person's privacy ends, the other's privacy begins. It also means that a person can independently shift the limits of their privacy, in a way they can protect it or they can disclose it to the public. Such observations relate to the concept of privacy and not to the concept of the right to privacy. The right to privacy is already an institutionally guaranteed human right, by means of which they can claim legal protection of his privacy. The terms privacy and the right to privacy are often confused and used as synonyms, which should be assessed negatively. Below, an attempt will be made to distinguish between these two concepts.

Concentrating on the concept of privacy at this point, it should be noted that a man basically has two spheres of life. The first of them is the public sphere, which is characterized by the fact that all designations included in it can be known by

43 Jędruszczak, 2005, pp. 111–135; Popiołek and Wieczorkowski, 2018, pp. 261–270; Jędrzej, 2014, pp. 1–4; Mider and Ziemak, 2021, pp. 132–172.

44 Sobczyk, 2009, pp. 299–318; Czopek, 2016, pp. 67–73; Kuczyński, 2009, pp. 30–32; Wiewiórowski, 2014, pp. 145–155.

other people. According to the *PWN Dictionary of the Polish Language,*[45] "public" means "concerning the whole society or some collective," "accessible or intended for all," "connected with some office or with some non-private institution" or "openly witnessed." However, according to the *Dictionary of the Polish Language* edited by W. Doroszewski [46] "public" means "affecting the public, not individuals; not being someone's personal property, intended for everyone; associated with some office, institution; universal, general, non-private, or happening in a place accessible to all, visible, accessible to the public; official, apparent." In the Polish legal literature, most publications on the public sphere of human life concern the right to public information, including its conflict with the right to privacy.[47] The right of access to public information has been guaranteed in Art. 61 of the Constitution of the Republic of Poland of April 2, 1997 (CRP).[48] On the other hand, the private sphere of human life stands in opposition to the public sphere. It can be reasonably stated that the private sphere includes all those designations that are intended solely for the attention of a specific group of individuals or for the knowledge of one specific individual. According to the *PWN Dictionary of the Polish Language* [49] "private" means "personally owned," "not under the control of the state or any public institution" or "relating to someone's personal and family matters." However, according to the *Dictionary of the Polish Language* edited by W. Doroszewski[50] "private" means "concerning someone personally, someone's personal matters, someone's personal property; not related to any institution, office, function, etc.; non-state, non-public, unofficial, domestic, unofficial ." This definition makes it clear that privacy is one side of the coin with the public being the other. It is not vital to establish the very fact of the difference between these concepts, as it is obvious. It is essential to establish the boundary between privacy and the public, and more precisely, it is necessary to select the factor determining this boundary. After analyzing the presented dictionary definitions and considering the already cited literature, it can be concluded that the private sphere is any manifestation of human activity that is not subject to disclosure based on generally accepted and enforceable rules in force in a given society. People forming national societies are subject to state jurisdiction, which defines rules and regulations in the form of universally binding law. The private sphere of human life is therefore a sphere not subordinated to public authority, which may introduce an order for an individual to disclose certain information, which, if not for this order, would remain in the sphere of private domain.

45 PWN Polish Language Dictionary. https://sjp.pwn.pl/sjp/publiczny;2573013.html.
46 Dictionary of the Polish Language edited by Doroszewski W. https://sjp.pwn.pl/doroszewski/publiczny;5487884.html.
47 Florczak-Wątor, 2019, p. 207; Sibiga, 2003, pp. 5–11; Michalak, 2016, pp. 47–65.
48 Constitution of the Republic of Poland of April 2, 1997 (Journal of Laws of 1997, No. 78, item 483, of 2001, No. 28, item 319, of 2006, No. 200, item 1471, of 2009, No. 114, item. 946.).
49 PWN Polish Language Dictionary. https://sjp.pwn.pl/sjp/prywatny;2572884.html.
50 Dictionary of the Polish Language edited by W. Doroszewski W. https://sjp.pwn.pl/doroszewski/prywatny;5482528.html.

In this way, certain information is no longer purely private information. However, this does not automatically mean that it becomes immediately publicly available. This leads to the conclusion that both the private and the public sphere have their own aspects. In the private sphere there is a personal aspect (information is known only to the person to whom it relates and no one else) and a limited horizontal aspect (information is known only to selected persons who have been voluntarily informed by the person to whom this information relates, and no one else). It is still possible to consider whether the unlimited horizontal aspect (the person whose information relates to voluntarily disclose it to the public) falls within the private sphere. In the presented division, the criterion of which is the disclosure orders provided for in the law, the unlimited horizontal aspect, although it may seem unintuitive, remains in the private sphere, because in this case the individual decides voluntarily to disclose information about it to the public.[51] On the other hand, the public sphere has a limited vertical aspect (information is known only to the person it concerns and the public authority) and an unlimited vertical aspect (public information). A visible *prima facie* difference is the entity which decides to extract information beyond the personal aspect of a person's private sphere. If the subject is a person to whom the information relates, the situation should be assessed as being in the sphere of privacy. On the other hand, if the decisive entity is the public authority, then such a situation should be assessed as falling within the public sphere. This leads to the conclusion that the sphere of privacy is determined by the sphere of the audience. In other words, what is not defined by law as falling under the public sphere is subject to the private sphere.

The right to privacy is a completely different issue. As the name suggests, this is an entitlement of an individual. An individual has the right to have his or her sphere of privacy respected and negatively respected by the state or other private entity, and if necessary, also guaranteed through positive actions. In international law, the right to privacy is provided for in many legal acts. Solely for example, in accordance with Art. 7 of the Charter of Fundamental Rights of the European Union (EU CFR)[52] "Everyone has the right to respect for his or her private and family life, home and communications.",[53] in accordance with Art. 17 of the International Covenant on Civil and Political Rights [54] "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of

51 Regardless of the fact of disclosing private information to the public, a person may subsequently change their decision and submit claims to respect his privacy. A good example is the right to be forgotten (see Skoczylas, 2018, pp. 87–100).

52 Charter of Fundamental Rights of the European Union (Journal U. UE. C. of 2007 No. 303, p. 1 as amended).

53 See Vested-Hansen, 2014, cited in Peers et al., 2014, pp. 153–183; Choudhry, 2014, cited in Peers et al., 2014, pp. 183–223.

54 International Covenant on Civil and Political Rights opened for signature in New York on December 19, 1966. (Journal of Laws 1977 No 38 item 167).

the law against such interference or attacks,"[55] according to Art. 8 Convention for the Protection of Human Rights and Fundamental Freedoms[56] "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.",[57] and according to Art 12. of Universal Declaration of Human Rights[58] "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[59] The cited provisions of international law are a good example of how the right to privacy is normatively treated. According to the international regulations, the elements of privacy are private, family, home, home, communication and correspondence. Nevertheless, these are only examples, although extremely broad, proving an open catalog of privacy designates, which is consistent with the previous comments made in this chapter. Additionally, the analysis of these provisions leads to the conclusion that the right to privacy is recognized as a law protecting against unjustified interference. This power is intended to guarantee that human privacy is respected and, in the event of a breach, that the state before the breach is restored or that the harm or damage will be repaired. This is why the right to privacy is, on the one hand, such an important point in every legal system, and on the other hand, its spectrum of impact does not refer only to one branch of law, it is a cross-sectional law. Provisions protecting human privacy can be found in many legal acts concerning various matters. Regardless, the function of this law is essentially clear. The right to privacy, although it is a typical right to something, is supposed to protect human privacy. Such a law is needed both horizontally and vertically. The protective function of the right to privacy can be distinguished into a protective function in the vertical aspect and a protective function in the horizontal aspect. The protective function in the horizontal aspect consists in ensuring that the sphere of privacy of a specific person will be protected against legally unjustified interference of another private entity (e.g., when a private entity wants to publish private data about a specific person without their consent; when a private entity wants to know private data about a specific person without their consent, but without the intention of making them public; when a

55 See Joseph and Castan, 2013, pp. 533–562.

56 The Convention for the Protection of Human Rights and Fundamental Freedoms was opened for signature in Rome on 4 November 1950, then amended by Protocols No.3, 5 and 8 and supplemented by Protocol No.2 (Journal of Laws 1993 no. 61 item. 284).

57 Nowicki, 2013, pp. 664–740.

58 *Universal Declaration of Human Rights*. https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf.

59 Rehof, 1999, cited in Alfredsson and Eide, 1999, pp. 251–265.

private entity extends the horizontal limited aspect of the private sphere of a specific person without their consent). The protective function in the vertical aspect, in turn consists in ensuring that the sphere of privacy of a specific person will be protected against unjustified interference by public authorities (e.g., when the public authority wants to make too much information public; when the public authority wants to know too much information about a specific person, but without making them public; when the public authority is unable to protect non-public information about a specific person). This distinction of the protective function of the right to privacy shows, on the one hand, how important this right is for every human being, and on the other hand, that its source is not only statutory law, but also the concept of natural law. This can be seen directly at the protective function in the vertical aspect. In the horizontal aspect, this is also the case, but it can be seen indirectly, because only through the prism of law established by public authority, which is subject to the rules of natural law. This is because the right to privacy belongs to every human being only because they were born as a human being, regardless of whether the statutory law confirms it or not.

Therefore, it is important at this point to indicate which factor should determine whether the interference in the sphere of human privacy is justified or unjustified. In the horizontal aspect, the decisive factor whether an interference by another private entity is justified or not is, in principle, the statutory law. However, it is different in the vertical aspect. It seems to be about maintaining a proper relationship between what is to remain private and what should be public. In this case, we are dealing with the weighing of at least two interests, where the sides of this weighing are of different nature. On one hand, there is always the aforementioned human privacy, which is of a static nature. On the other hand, there may be many other interests of a dynamic nature, such as public security, the economic well-being of the country, protection of order and crime prevention, health protection, morality, protection of rights and freedoms other than the right to privacy. In this case, what determines the legitimacy of the interference with someone's privacy is the principle of proportionality. The tool of the proportionality principle is the proportionality test. In fact, it is the proportionality test that determines whether a vertical interference in the sphere of human privacy is justified or unjustified. In many legal orders, the proportionality test is used as a normatively defined measure of the justification of legal solutions within which valuable interests collide. An example of such a legal system is the law of the EU,[60] where it is indicated that a legal measure meets this test when it enables the achievement of a legitimate goal, it is the least onerous measure of all measures enabling the achievement of this goal and is characterized by a commensurate balance between legal costs and inconvenience for the individual and the importance of the goal it pursues.[61] In other

60 This rule currently results from Art. 5 sec. 4 TEU, as well as Art. 52 sec. 1 of the EU Charter (See Emiliou, 1966, p. 320; Długosz, 2017, pp. 283–300; Jacobs, 1999, cited in Elllis, 1999, pp. 1–23).

61 Gekiere, Baeten and Palm, 2010 cited in Mossialos et al., 2010, pp. 506–508.

words, this means that the restrictive measure meets the requirements of the proportionality test only if it is appropriate, necessary and proportionate in the strict sense.[62] The same should be true for legal measures by public authority restricting human privacy.

Considering the observations presented so far, it is possible now to try to provide a definition of the right to privacy. Thus it seems that, the right to privacy is the right of every human being, belonging to them only because they are a human being (element of natural law), to be sure that in their sphere of privacy (e.g., private, family, home, home, communication, correspondence), there was no legally unjustified (horizontal aspect) or unjustified by the proportionality test (vertical aspect) interference (protective function) of another private entity or state (positive and negative actions), and in the case of unjustified violation of privacy, that the state from before the violation will be restored or that harm or the damage that has been caused will be repaired. The presented definition of the right to privacy has the advantage that it quite precisely defines the material scope of this right, its sources and functions, considering also the multi-component nature of the analyzed term and its various aspects. It also seems that the realities of digital reality should not affect the essence of the right to privacy, the guiding direction of its understanding- in other words, to the proposed definition. What is changing is the subjective scope of the private sphere of each person, as it is expanding with emerging designations of technical, technological and civilization progress (e.g., a social media account). The environment within which the right to privacy should protect people's privacy is changing, too. This means that the legal means of the right to privacy should be appropriate from the point of view of the aforementioned features of cyberspace, and should be accordingly adapted. This leads to the conclusion that practically the most important now is to perform usability analysis of specific legal instruments protecting privacy not only in the traditional world, but also in the digital sphere. This is because the digital reality is changing much faster than the traditional world and in the digital world human privacy is much more exposed to unjustified interference, most often in a horizontal aspect. Therefore, the scope, content and form of legal measures to protect privacy today should be, firstly, appropriate to the purpose of this protection, both in the traditional and digital world, and, secondly, it should be constantly updated and consider the changes taking place in cyberspace due to technical, technological and civilization progress.

After presenting the observations on terminological issues, to fulfill the purpose of this study, it is necessary now to present the properly understood right to privacy in Polish law, considering the specificity of digital reality as a new place for human privacy.

62 Golec, 2018, pp. 162–163.

## 4. The right to privacy in the Constitution of the Republic of Poland

There is a normatively defined right to privacy in the CRP. Within the framework of the CRP systematics, a legal norm can be distinguished, which in this respect is of a basic nature. Namely, in accordance with Art. 47 CRP Everyone shall have the right to legal protection of one's private and family life, of one's honor and good reputation and to make decisions about his personal life. According to the judgment of the Polish Constitutional Tribunal (PCT) of 5 March 2013,[63] the provision cited provides for two separate rights of the individual. The first entitlement is the right of an individual to legal protection of the spheres of life indicated in this provision. The second is the freedom to decide on matters related to your personal life. According to the Constitutional Tribunal, the first law must be accompanied by a statutory regulation to defend privacy, family life, honor and good name. The second law, on the other hand, in fact prohibits interference with the freedom to decide about one's personal life. Importantly, it is these two constitutional norms contained in the cited provision of the Constitutional Tribunal law that are defined as the right to privacy. It is also noted that at the constitutional level in Poland, privacy is protected in many aspects, including by more detailed provisions, i.e., Arts. from 48 to 51 CRP.[64] The legal norms contained therein constitute the next aspects of the entitlement provided for in Art. 47 CRP. According to Art. 48 CRP:

> 1. Parents shall have the right to rear their children in accordance with their own convictions. Such upbringing shall respect the degree of maturity of a child as well as his freedom of conscience and belief and also his convictions. 2. Limitation or deprivation of parental rights may be effected only in the instances specified by statute and only based on a final court judgment.[65]

Art. 49 CRP:

> The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute.[66]

Art. 50 CRP:

> The inviolability of the home shall be ensured. Any search of a home, premises or vehicles may be made only in cases and in a manner specified by statute.[67]

63 See Verdict of the Constitutional Tribunal of 5 March 2013, file ref. act U 2/11.
64 See Verdict of the Constitutional Tribunal dated December 12, 2005, file ref. act K 32/04.
65 See Verdict of the Constitutional Tribunal of December 2, 2009, file ref. act U 10/07.
66 See Verdict of the Constitutional Tribunal of 30 July 2014, file ref. no. K 23/11.
67 See Decision of the Supreme Court of December 18, 2019, file ref. no. V CSK 347/19.

Art. 51 CRP:

> 1. No one may be obliged, except based on statute, to disclose information concerning his person; 2. Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law; 3. Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute; 4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute; 5. Principles and procedures for collection of and access to information shall be specified by statute.[68]

As can be seen, the quoted regulation is a more detailed constitutional approach to the privacy of every human being in Poland with issues related to parental right, confidentiality of communication, inviolability of the home and the right to personal data protection. All these topics constitute a detailed aspect of the privacy of every human being, which has its general source in Art. 47 CRP. This means that in the taxonomy of the CRP, Art. 47 is of great importance as it confirms that every human being has the right to privacy. In other words, it underlines the fact that a right derived from natural law is respected by the public authority. Additionally, this observation is confirmed by the fact that under Polish constitutional law, the interests referred to in Art. 47 CRP, are protected by the so-called non-derogatory rights, i.e., those that cannot be limited even under martial law and a state of emergency, as evidenced by the content of Art. 233 para. 1 CRP.[69] Turning to the legal protection measures provided for in the CRP, it should be noted that there are several important legal norms in this respect in Polish constitutional law. It should be emphasized that this regulation is fully applicable in the field of legal protection of the right to privacy. First, according to Art. 77 of the CRP, everyone has the right to compensation for the damage caused to him by unlawful action of a public authority, and statutory law may not prevent anyone from seeking the infringed rights or freedoms.[70] Secondly, according to Art. 78 of the CRP, each party has the right to appeal against judgments and decisions issued in the first instance.[71] Third, in accordance with Art. 79 of the CRP, everyone whose constitutional freedoms or rights have been violated has the right, under the terms of the Act, to lodge a complaint with the Constitutional Tribunal on the compliance with the CRP of the act or other normative act, based on which the court or public administration body finally adjudicated on his freedoms or rights or about his obligations set out in the CRP.[72]

68 See Verdict of the Constitutional Tribunal of 13 December 2011, file ref. act K 33/08.
69 See Verdict of the Constitutional Tribunal dated October 30, 2006, file ref. no. P 10/06.
70 See Verdict of the Constitutional Tribunal of July 1, 2021, file ref. no. SK 23/17.
71 See Verdict of the Constitutional Tribunal of October 30, 2019, file ref. act P 1/18.
72 See Verdict of the Supreme Court of February 20, 2018, file ref. no. V CSK 230/17.

Fourth, in line with Art. 80 CRP everyone shall have the right to apply to the Commissioner for Citizens' Rights for assistance in protection of his freedoms or rights infringed by organs of public authority.[73] The indicated constitutional regulation is the basic catalogue of legal protection measures in Poland. The fact that they were foreseen in the CRP emphasizes that the intention of the constitutional legislature in Poland was to equip every person with real instruments to protect him against the actions of the ordinary legislature. It also means that the presented catalog of constitutional measures for the protection of rights and freedoms is fundamental and, in principle, inviolable. Other legal protection measures are provided for in individual branches of statutory law. Regardless, however, the constitutional right to privacy is not an absolute right that cannot be limited. In the light of Art. 31(3) of the CRP, there is a possibility of introducing restrictions on the right to privacy, but they must be established only by statute and only if they are necessary in a democratic state for its safety or public order, or for the protection of the environment, public health and morality, or freedom and the rights of others. These restrictions must not infringe the essence of the right to privacy. On the other hand, when assessing the usefulness and importance of the provisions of the CRP in the field of privacy protection in digital reality, it should be emphasized that due to the abovementioned arguments and considering the highest position of the CRP in the Polish legal system, the importance of this regulation in digital reality is the same as in the traditional reality. It can be neither greater nor smaller, since this significance is, as has already been indicated, fundamental. This is the highest-level guarantee that an individual can always count on legal protection of their rights and freedoms. The same should be said about the usefulness of these legal measures in the digital environment. There is no reason to argue that these legal means are losing their effectiveness as a result of technical, technological or civilization progress. It can even be said that the norms provided for in the CRP are resistant to such factors, and rightly so, because regardless of the features of cyberspace, they must be equally applicable. This may mean the necessity to be open to the application of a broader interpretation of certain aspects of legal remedies from the CRP. It seems, however, that it is permissible as it is to the advantage of the protected entity. It would be unacceptable the other way, so when it would be necessary to interpret narrowly. The extension of the constitutional protection of rights and freedoms with new designations related to cyberspace should be assessed positively. As mentioned above, people bring their rights and freedoms to cyberspace, including this kind of legal protection measures. Under these conditions, or in the context of these conditions (e.g., cyberspace law), constitutionally defined protection must work just as well as it does in the traditional world. What is naturally changing is the actual state of affairs in the context of which a constitutional legal protection measure may be launched. In other words, both in the traditional and digital world, the aforementioned legal measures must function as intended.

73 See Zieliński, 2021, p. 23.

## 5. The right to privacy in civil law

The main legal act of civil law in Poland is the Act of 23 April 1964—Civil Code (the Civil Code).[74] According to Art. 23 of the Civil Code, Personal property of man, as in particular health, freedom, honor, freedom of conscience, surname or pseudonym, image, secret of correspondence, inviolability of an apartment, scientific, artistic, invention and rationalization, remain under the protection of civil law, irrespective of the protection provided for in other legislation. .[75] Personal goods are values recognized by the legal system that include the physical and mental integrity of a human being, as they constitute an attribute of every natural person with whom they are closely related and as such have an individual character and are protected by the construction of subjective rights of an absolute nature..[76] It is significant that the indicated catalog of personal rights is open .[77] In accordance with the relevant case law, the open catalog of personal rights also includes personal rights related to the sphere of private and family life and the area of intimacy .[78] Protection in this respect may relate to cases of disclosure of facts from personal and family life, abuse of information obtained, collecting information and assessments from the sphere of intimacy through private interviews to publish them or otherwise disseminate them.[79] According to Art. 24 of the Civil Code he person who is in danger of being threatened by another person may be required to refrain from doing so unless it is not unlawful. In the event of an infringement, he may also require that the person who has committed the infringement has completed the steps necessary to remove the effects thereof, in particular to make a statement of the relevant content and in an appropriate form. Based on the principles laid down in the Code, it may also require the payment of monetary or payment of an appropriate amount of money to a designated social objective. Although, as noted in the jurisprudence, not every breach of the right to privacy justifies the demand for pecuniary compensation for the harm suffered. .[80] If, as a result of a breach of the personal property, damage to the property has been caused, the victim may be required to remedy it on a general basis. Importantly, Art. 24 of the Civil Code does not prevent the exercise of rights provided for in other provisions of Polish law. According to the relevant jurisprudence, an unlawful infringement of a personal interest may occur both through the public formulation of false allegations, slander, providing data and information from

74 Act of 23 April 1964 — Civil Code (i.e., Journal of Laws of 2021, item 1509, as amended).
75 Wojcieszak, 2021, pp. 701–720.
76 Verdict of the Supreme Court of May 26, 2017, file ref. no.I CSK 557/16.
77 Decision of the Supreme Court of December 17, 2021, file ref.no. I CSK 226/21.
78 Verdict of the Supreme Court of July 17, 2020, file ref. act III CSK 6/18; Judgment of the Supreme Court of January 18, 1984, file ref. no. I CR 400/83; Judgment of the Supreme Court of May 11, 2007, file ref. no. I CSK 47/07; Resolution of the Supreme Court of May 28, 2021, file ref. act III CZP 27/20.
79 Verdict of the Supreme Court of January 18, 1984, file ref. no. I CR 400/83; Verdict of the Supreme Court of 8 July 2011, file ref. IV CSK 665/10.
80 Verdict of the Supreme Court of May 5, 2021, file ref. act I NSNc 156/20.

the sphere of private life (in particular intimate life), insult, etc., as well as through a statement addressed to the person concerned himself, to the sphere of whose personal rights the interference occurs.[81] Importantly, the provision of Art. 24 of the Civil Code authorizes to submit claims as to whose personal rights were threatened with infringement or infringed .[82] The above is supplemented by Art. 448 of the Civil Code, according to which in the event of a breach of a personal good, the court may grant to that person whose personal good has been infringed, the corresponding sum of the degree of redress for the injured or at his/her request the corresponding amount of money to be indicated by the court or tribunal of the General Court. the social objective, irrespective of any other means needed to remove the effects of the infringement .[83] It is worth emphasizing that the content of this provision shows that even in the event of violation of a personal interest, the court may, but does not have to, award compensation.[84] However, the court's discretion in this respect is limited, which means that it must provide a legally relevant reason for the refusal to award a claim resulting from the specific circumstances of the case, despite meeting the statutory conditions.[85] Such reasons are, in particular, the negligible dimension of the harm, the perpetrator's reflection on himself and his voluntary efforts to compensate for this harm, as well as the minor causal share of the perpetrator's behavior in causing non-pecuniary damage.[86] For example, Polish jurisprudence recognizes that disclosure of financial conflicts in the family or conducting criminal proceedings in a case of domestic violence and confidential information regarding divorce is a violation of the right to privacy.[87] However, as it was also emphasized in the relevant jurisprudence, not every unpleasantness constitutes a violation of personal interests and is subject to compensation in the regime of protection of personal rights, and the legal system does not guarantee freedom from stress and unpleasantness related to life events.[88] Referring at this point to the usefulness and importance of these provisions in the digital reality in the context of the right to privacy, it should be noted that the norms of Polish civil law mentioned above can successfully find and

81 Verdict of the Supreme Court of May 17, 2019, file ref. no. IV CSK 79/18.
82 Verdict of the Supreme Court of September 21, 2006, file ref. no.I CSK 118/06.
83 See Verdict of the Court of Appeal in Warsaw of January 3, 2022, file ref. no. I ACa 354/21.
84 Resolution of the Supreme Court of October 18, 2011, file ref. act III CZP 25/11.
85 Verdict of the Supreme Court of May 5, 2021, file ref. act I NSNc 156/20.
86 Verdict of the Supreme Court of 23 January 1974, file ref. II CR 763/73; Verdict of the Supreme Court of June 13, 2002, file ref. act V CKN 1421/00; Verdict of the Supreme Court dated April 19, 2006, file ref. no. II PK 245/05; Verdict of the Supreme Court of September 24, 2008, file ref. no. II CSK 126/08; Verdict of the Supreme Court of June 3, 2011, file ref. act III CSK 279/10; Verdict of the Supreme Court of 5 July 2012, file ref. act IV CSK 603/11; Verdict of the Supreme Court of November 27, 2014, file ref. no. IV CSK 112/14; Verdict of the Supreme Court dated December 16, 2014, file ref. no. I PK 124/14; Verdict of the Supreme Court of August 20, 2015, file ref. no. II CSK 595/14; Verdict of the Supreme Court of March 6, 2019, file ref. no. I CSK 88/18.
87 Verdict of the Supreme Court of January 18, 1984, file ref. no. I CR 400/83; Verdict of the Supreme Court of December 6, 1990, file ref. no.I CR 575/90.
88 Resolution of the Supreme Court of November 19, 2010, file ref. act III CZP 79/10; Supreme Court verdict of 7 December 2011, file ref. II CSK 160/11.

generally apply in cyberspace conditions. These regulations, as indicated, are very broadly defined. This is evidenced by the fact that although privacy was not *expressis verbis* mentioned as one of a person's personal rights, as a result of the application of a dynamic interpretation, it became a personal good. Thus, the provisions of Art. 23, 24 and 448 of the Civil Code can successfully play a significant role in the protection of privacy in the age of applying modern technologies for practical use.

In Poland, civil law remedies are gaining popularity due to their effectiveness. This effectiveness is high when it comes to the realities of the traditional world. However, it is different in the digital reality. Here we have at least three big issues. The first problem is the widespread anonymity of cyberspace users. Therefore, if someone violates the privacy of another person in cyberspace, to effectively benefit from the legal protection provided for in civil law, it is necessary to determine the personal data of the infringer. In this context, it can be said, however, that the current possibilities of ICT detection techniques are wide, although unfortunately not very well known. Therefore, a possible solution to this problem could be not only to provide civil courts with the power to effectively abolish anonymity of cyberspace users, but also to make the public aware of this fact. The second problem is the difficulty in determining the law applicable in the event of violating someone's privacy in cyberspace. We are talking here about the application of legal meta-norms, which would clearly indicate, for the benefit of the weaker party, the principles of establishing an appropriate legal regime under which one can assert their rights. In the era of digitization, this is a big problem, because the person who violates privacy may be from Canada, and the person whose privacy is violated may be from Portugal. And to make things even more complicated, the breach of privacy takes place on a social network registered in the Dominican Republic. A remedy for this problem would be to define common rules for determining the applicable law. A third problem related to the second one mentioned above is the difficulty in determining jurisdiction in cyberspace. This difficulty is due to the same reasons as the problem of the applicable law. A solution to this problem would also be to define common rules for determining the competent jurisdiction. After eliminating these problems, in principle, the protection of privacy in Polish civil law would be as effective and predictable as in the traditional world.

## 6. The right to privacy in criminal law

It is different in case of the criminal law than in civil law. Here, human privacy is protected based on penalizing violations of a legally protected good. This means that legal remedies in criminal law are specific types of prohibited acts. In turn, the procedural criminal law plays a role that enables the fulfillment of the purpose of a specific legal protection measure of Polish criminal law. In Poland, the basic

legal acts in this area are the Act of June 6, 1997—Penal Code (PPC)[89] and the Act of June 6, 1997—Code of Criminal Procedure (CoCP).[90] In this way, in Poland, as in most modern countries, one can distinguish between substantive criminal law and procedural criminal law.

There are several types of prohibited acts in Polish substantive criminal law, which can be associated with the pursuit of repressive protection of human privacy. The basic and most important provision of Art. 267 of the PPC, according to which:

> §1. Whoever without authorization gains access to information not intended for him, by opening a closed letter, connecting to the telecommunications network or breaking or bypassing electronic, magnetic, IT or other special security thereof, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to two years. §2. The same penalty shall be imposed on anyone who gains access to all or part of the IT system without authorization. §3. The same penalty shall be imposed on anyone who, to obtain information to which they are not entitled, puts on or uses a tapping device, visual device or other device or software. §4. The same penalty shall be imposed on anyone who discloses the information obtained in the manner specified in §1-3 to another person. §5. The prosecution of the offense specified in §1-4 takes place at the request of the injured party.

This provision implements Art. 2 and 3 of the Convention on Cybercrime by Council of Europe [91] to the Polish normative order. The act that fulfills the statutory features of this crime will most often be behavior that violates someone's privacy. According to Polish jurisprudence, under Art. 267 §1 PPC, only such a set of signs that can be assigned a specific meaning should be considered as information.[92] Thus, the essence of the offense referred to in Art. 267 PPC, is to obtain discretionary information, not intended for the perpetrator.[93]. Another overtone is gaining access to information or an IT system, which pursuant to Art. 267 §2 PPC is punishable when the perpetrator does not have the right to do so, i.e., it is illegal, violating the right of another entity to dispose of information or to obtain it.[94] However, the norm contained in Art. 267 §3 PPC ensures protection of the statements of the participants of the conversation, if at least implicitly they made them confidential, and the intentions that determined the status of the speech are irrelevant here.[95] On the other hand, the device referred to in that provision is any device used to record an image

89 Act of 6 June 1997 — Penal Code (consolidated text Journal of Laws of 2021, item 2345, as amended).
90 Act of 6 June 1997 — Code of Criminal Procedure (consolidated text Journal of Laws of 2022, item 655, as amended).
91 The Council of Europe Convention on Cybercrime, drawn up in Budapest on November 23, 2001 (Journal of Laws of 2015, item 728); McQuade, 2009, p. 46; Clough, 2010, p. 50.
92 Decision of the Supreme Court of March 5, 2019, file ref. no. II KK 208/18.
93 Verdict of the Supreme Court of March 24, 2004, file ref. act IV KK 46/04.
94 Verdict of the District Court in Wałbrzych of September 23, 2016, file ref. no. III K 865/15.
95 Decision of the Supreme Court of 27 April 2016, file ref. no. II KK 265/15.

or sound, i.e., an analog or digital device intended for this purpose, e.g., a camera, voice recorder .[96] This means that in the light of the above, the unlawful installation of a device for obtaining information about the driving route and thus the location of a given person in someone else's vehicle is prohibited and constitutes a prohibited act.[97] Other provisions of the Penal Code, which can also be classified as aiming at repressive protection of human privacy, are Arts. 268 (Destruction of information), 268a (Damage to databases), 269 (Computer sabotage), 269a (disruption of work on a network), 269b (legal use of computers and data) and 270 §1 (Forgery). When assessing the above-mentioned provisions of Polish substantive criminal law from the perspective of measures to protect privacy in cyberspace, it should be emphasized that in Poland there is a modern law in this area in place. This is mainly due to the good implementation of the Convention on Cybercrime by the Council of Europe. The legal norms discussed above are a real weapon in the fight against cybercrime, which is undoubtedly one of the most important threats to privacy in the era of modern technologies put into practical use. As a rule, the current legal regulations of Polish substantive criminal law should be assessed as effective in terms of the repressive protection of privacy and clearly indicating what acts against human privacy should be considered forbidden in cyberspace, i.e., cybercrimes. There are many guarantees of respect for human privacy in Polish procedural criminal law. This is because, as part of the criminal process, there are numerous restrictions on the rights and freedoms provided for, for example, in the CRP. One of the rights that are reduced in the CoCP is the right to privacy. It seems to be a natural effect of the pursuit of the fulfillment of the subject of Polish criminal proceedings, i.e., in principle,[98] to establish the legal liability of the accused for the alleged offense.[99] This determination of the legal responsibility of the accused for the alleged offense often requires, even as part of evidentiary proceedings, state interference with the rights and freedoms of persons, and it seems that the right to privacy in particular. This interference causes a normative limitation of the scope of the right to privacy, and thus reduces the protection of privacy, which causes that more designations of the private sphere of a person, than under non-criminal-procedural conditions, are transferred to the public sphere. This is because, as indicated, the right to privacy is not an absolute right and is subject to limitations, but in strict accordance with Art. 31 (1) of the CRP. This means that the right to privacy may be legally limited for the purposes of criminal proceedings, but the essence of the right to privacy cannot be violated. Process guarantees of respecting privacy, as specific penal-procedural means of protecting privacy, are therefore aimed at ensuring that this essence is not violated. The CoCP provides for rules governing the taking of evidence of a search,

96 Decision of the Supreme Court of 27 April 2016, file ref. act III KK 265/15.

97 Decision of the Supreme Court of November 27, 2019, file ref. act V KK 505/1.

98 See Bennecke and Beling, 1900, p. 202; Sauer,1951, p. 103; Schmidt, 1952, p. 43; Beling, 1928, p. 5; Birkmeyer, 1898, pp. 63–67; Rosenfeld, 1909, p. 23; von Kries, 1892, pp. 4–5.

99 See Schaff, 1959, p. 255; Cieślak, 1959, p. 246; Daszkiewicz, 1985, p. 33; Bieńkowska, 1994, p. 67.

which provide for guarantees of respect for privacy. We are talking here in particular about Art. 220 (search—authorized body, approval), Art. 221 (search hours), Art. 223 (search of a person), Art. 224 (method of conducting the search) of the CoCP. Art. 227 of the Code of Criminal Procedure is of significance here, according to which Searching or seizing objects shall be conducted in accordance with the objective of the action, with moderation and respect for the dignity of the persons to whom the action relates, and without unnecessary damage or hardship.[100] The Polish CoCP also provides for provisions on the control and recording of conversations, where there are also certain guarantees of respecting human privacy. They take place in Art. 237 (Admissibility), Art. 238 (Duration) and Art. 240 (Interlocutory appeal) of the CoCP. In terms of protecting the essence of the right to privacy, the prohibitions on evidence, in particular in Art. 178 (prohibition of questioning a defense counsel and a clergyman), Art. 182 (Refusal to testify), Art. 185 (Release from obligation to testify) and Art. 199 (Inadmissibility of evidence). The legal norms cited above relate to the taking of evidence. Here, in terms of privacy protection, it is about maintaining the proportion between two important interests, namely the realization of the value of truth and the protection of the privacy of every human being. The purpose of criminal proceedings is to establish the legal responsibility of the accused for the alleged offense, and for this purpose the evidence is collected, including due to the current technical and technological progress, also electronic evidence. This possibility results directly from Arts. 218a and 236a of the CoCP.[101] Therefore, data related to the needs of criminal proceedings is processed here. Referring to the usefulness and importance of legal measures to protect human privacy in Polish criminal proceedings, it should therefore be stated that there was a need to define the appropriate rules for the processing of data obtained as part of evidence proceedings. It should

100 Pikul, 2012, pp. 161–170.

101 According to Art. 218a of CoCP, "§1. Offices, institutions, and entities carrying out telecommunications activities or supplying electronic services and providers of digital services are under an obligation to immediately secure, upon demand of a court or a public prosecutor contained in a decision, for a specific period of time not longer than 90 days, IT data stored on devices containing such data on a carrier or in an IT system. In cases concerning offences referred to in Articles 200b, 202 § 3, 4, 4a, 4b or Article 255a of the Criminal Code and in Chapter 7 of the Act of 29 July 2005 on Counteracting Drug Addiction (Dziennik and Ustaw 2020, item 2050, of 2021, item 2469 and of 2022, items 763 and 764), the obligation to secure data mentioned above may be combined with the obligation to prevent access to these data. The provision set out in the second sentence of Article 218 § 2 shall apply accordingly. §2. IT data referred to in § 1, irrelevant to the criminal proceedings, shall be immediately released from such security measures. §3. The provisions of § 1 and 2 shall apply accordingly to securing contents published or made available electronically, with the stipulation that the entity obliged to enforce the demand made by a court or public prosecutor may also be the controller of these contents. § 4. If the publication or granting of access to contents referred to in § 3 was a prohibited act as referred to in § 1, the court or public prosecutor may order the deletion of the said contents and impose an obligation to execute the decision on entities referred to in § 1 or § 3."; According to Art. 236a of CoCP, "The provisions of this chapter apply accordingly to the administrator and user of a device containing IT data or of an IT system, in the scope of data stored on that device or in that system, or on a carrier administered or used by such a person, including e-mail correspondence."."

be emphasized that such a need existed, as the Act of December 14, 2018 on the protection of personal data processed in connection with the prevention and combating of was passed relatively recently in Poland.[102] The Act of December 14, 2018 defines the rules and conditions for the protection of personal data processed by competent authorities for the purpose of identifying, preventing, detecting and combating prohibited acts, including threats to public safety and order, as well as performing pretrial detention, penalties, and order penalties and coercive measures resulting in deprivation of liberty; the rights of persons whose personal data are processed by competent authorities and the legal remedies available to these persons; the manner of supervising the protection of personal data processed by competent authorities, with the exception of personal data processed by the prosecutor's office and courts; tasks of the supervisory body and the form and manner of their implementation; obligations of the administrator and processor as well as the data protection officer and the procedure for his appointment; method of securing personal data; the mode of cooperation with supervisory authorities in other EU countries; criminal responsibility. The most interesting from the point of view of the title issue are the provisions of Art. 50 (complaint against unlawful processing of personal data or notification of a violation of the processing of personal data), Art. 51 (complaint to the administrative court against the decision of the President of the Office or his inactivity in the matter of a complaint against unlawful processing of personal data or notification of a violation of personal data processing), Art. 52 (authorization of a social organization to exercise rights related to the protection of personal data), Art. 53 (compensation or compensation due from the administrator) of the Act of December 14, 2018. The Act of December 14, 2018 and the presented provisions of the CoCP seem to be adequate protection of human privacy based on criminal procedural law in the digital age.

## 7. The right to privacy in administrative law (personal data protection)

Most often, when the right to privacy or legal protection of privacy in administrative law is discussed, these considerations concern the protection of personal data.[103] Personal data protection in the age of applying modern technologies for practical use is becoming one of the most popular legal issues. This fact is evidenced by the countless number of scientific publications devoted to the multi-faceted analysis

102 Act of December 14, 2018 on the protection of personal data processed in connection with the prevention and combating of crime (Journal of Laws 2019, item 125).

103 Kręcisz-Sarna, 2018, pp. 199–213; Niczyporuk, 1999, pp. 29–35.

of this issue.[104] These are extremely interesting topics that require scientific research. It even seems that it is not an exaggeration to say that in today's digital world the protection of personal data is for many a synonym of their right to privacy, protection of privacy or privacy itself. Obviously, this is the wrong approach. Personal data is one of the pillars of privacy, one of its aspects. In turn, the protection of personal data is one of the pillars of privacy protection. Therefore, the right to the protection of personal data is one of the pillars of the broadly understood right to privacy. On the other hand, it is correct to say that today it is hard to imagine the protection of human privacy without the protection of personal data. The reason is the massive processing of such data. Nevertheless, Poland, like most European countries, is an EU member state. Under EU law, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)[105] and Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No 1247/2002 / EC.[106] Due to the fact that these are EU regulations, they have direct effect in the national legal systems of the EU Member States. This means that it is the law that Polish citizens can rely on directly. Therefore, in the field of personal data protection, there has been a certain unification of law at the EU level, as the EU regulation does not need to be implemented into the national legal order. This has a positive effect. Namely, a uniform approach to the protection of personal data in the EU increases the effectiveness of the enforcement of the introduced rules for the processing and administration of personal data. This is because in the event of non-compliance with the provisions of the GDPR, the entity violating the protection of personal data must consider a conflict with the entire EU market. It is not just one country, but already twenty-seven. It seems to be a powerful influence. Nevertheless, it results in the loss of the specificity of the national approach to the protection of personal data. Art. 8 of the EU CFR, according to which everyone has the right to the protection of personal data concerning them. Art. 8 of the EU CFR also stipulates that these data must be processed fairly for specific purposes and with the consent of the person concerned or on some other legitimate basis provided for

104 Just for example Drozd, 2004, pp. 25–31; Mezglewski, 2007, pp. 5–21; Gersdorf, 2005, pp. 14–19; Hucał, 2017, pp. 185–222; Mednis, 2018, pp. 85–103; Borowicz, 2001, pp. 2–11.

105 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1–88).

106 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45 / 2001 and Decision No 1247/2002 / EC (OJ L 295, 21.11.2018, pp. 39–98).

by law. In Poland, however, one can speak of a specific national, although due to the GDPR limited, approach to the protection of personal data. This is because the Act of May 10, 2018 on the protection of personal data was adopted in Poland. The Act on the Protection of Personal Data specifies: public entities obliged to appoint a data protection officer and the procedure for notifying about his appointment; the conditions and procedure for accreditation of the entity authorized to certify in the field of personal data protection, the entity monitoring the code of conduct and certification; the procedure for approval of the code of conduct; the authority competent for the protection of personal data; proceedings in the case of infringement of provisions on the protection of personal data; the mode of European administrative cooperation; monitoring compliance with the provisions on the protection of personal data; civil liability for violation of the provisions on the protection of personal data and court proceedings; criminal liability and administrative fines for violating the provisions on the protection of personal data. It seems that the purpose of this legal regulation is to support and strengthen the application of the GDPR in Poland. In the scope of legal protection measures contained in the Personal Data Protection Act, attention should be paid to Art. 92. Pursuant to this provision, to the extent not regulated by the GDPR, claims for infringement of the provisions on the protection of personal data referred to in Art. 79 and Art. 82 of the GDPR,[107] the provisions of the Civil Code shall apply, i.e., the above-mentioned regulations regarding personal rights. When

107 According to Art. 79 of the GDPR: 1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation. 2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. [2]Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers." According to Art. 82 GDPR: „1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. 2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. 2A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. 3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. 4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject. 5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2. 6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).”..”.

assessing the importance and usefulness of these provisions in the digital age, one should refer to the view expressed in the context of the right to privacy in civil law.

## 8. Conclusions

To sum up, this study presents the right to privacy in the digital age as fully as possible from the perspective of the Polish normative system with general theoretical elements. First, the discussion on digital reality as a new space for the right to privacy was presented. Second, an attempt was made to define the right to privacy. Third, the right to privacy has been shown in the light of constitutional regulations. Fourth, the right to privacy in civil law was presented. Fifth, the right to privacy in criminal law and trial was discussed. Sixth, the right to privacy in administrative law was presented. It is pointless to repeat the conclusions developed, which are visible in the earlier parts of this study. Nevertheless, it is purposeful to present three more conclusions that can be drawn.

First, human privacy is mirrored in the digital reality. Privacy does not change or disappear as a result of the emergence of modern solutions in the 21st century. Privacy must be protected within established limits, regardless of the environment of human activity. Wherever there is man, there is their privacy, and where there is privacy, there is the right to privacy and the protection of privacy.

Second, although everyone knows that they have their privacy, it is extremely difficult to define it. Everyone knows they have a right to privacy, but figuring out what it is a very difficult task. As part of the considerations contained in this study, the concept of privacy was addressed and a theoretical definition of the right to privacy was presented. In its context, it should be added that it is pointless to introduce it into the legal system as a legal definition. Such terms should be decoded in legal literature or jurisprudence. Introducing a definition in the law of a closed nature would limit the dynamic interpretation open to new designations of technical, technological and civilization progress. On the other hand, the introduction of an open definition of the right to privacy would not dispel interpretational doubts.

Third, there are many provisions on the right to privacy in the Polish legal system. We are talking about constitutional law, civil law, criminal law and administrative law. The legal measures contained in these branches of law should generally be assessed positively as passing the test of legal protection of human privacy. Apart from the indicated problems, their significance and usefulness in the digital age should also be assessed positively. Nevertheless, a certain observation arises regarding the effectiveness of domestic law. This efficiency within the boundaries of statehood in the traditional world is at an appropriate level. On the other hand, in the digital world without barriers to state borders and accepting universal anonymity, it seems that the effectiveness of national law is lower than that of common law for more

countries. This is best seen in situations where the entity responsible for the right to privacy is an entity such as transnational corporations or a social media manager. It therefore seems that international cooperation is the key to fighting for human privacy in the digital age.

Finishing this study, it should be strongly emphasized that all designations of modern technologies put into practical use should be created and implemented for the people and with people in mind. Man, in turn, has his rights and freedoms that should be enforced regardless of where the person is functioning. Therefore, respect for the right to privacy should be one of the conditions for the admissibility of applying modern solutions.

# Bibliography


Afsarmanesh, H., Masís, V. G., Hertzberger, L. O. (2004) 'Virtual Community Support in Telecare' in Camarinha-Matos, L. M., Afsarmanesh, H. (eds.) (2004) *Processes and Foundations for Virtual Organizations. PRO-VE 2003. IFIP — The International Federation for Information Processing*. 1st edn. Boston: Springer, pp. 211–220; https://doi.org/10.1007/978-0-387-35704-1_22.

Alfino, M., Mayes, R. G. (2003) 'Reconstructing the Right to Privacy', *Social Theory and Practice,* 29(1), pp. 1–18 [Online]. Available at: https://doi.org/10.5840/soctheorpract20032915 (Accessed: 24 October 2022).

Antoš, M. (2019) 'The Constitutional Right To Information In The Czech Republic: Theory And Practice', *International Comparative Jurisprudence*, 5(1), pp. 47–55 [Online]. Available at: https://doi.org/10.13165/j.icj.2019.05.006 (Accessed: 24 October 2022).

Arai, Y. (1998) 'The Margin of Appreciation Doctrine in the Jurisprudence of Article 8 of the European Convention on Human Rights', *Netherlands Quarterly of Human Rights,* 16(1), pp. 41–61 [Online]. Available at: https://doi.org/10.1177/092405199801600104 (Accessed: 24 October 2022).

Arwid, M. (2018) 'Ochrona danych genetycznych jako danych osobowych', *Studia Iuridica*, 2018(73), pp. 85–103 [Online]. Available at: https://bibliotekanauki.pl/articles/902483 (Accessed: 27 October 2022).

Băncilă A. M. (2018) 'Cyberspace – The New Dimension of Human Interaction', *Scientific Bulletin*, 23(1), pp. 5–10 [Online]. Available at: https://doi.org/10.2478/bsaft-2018-0001 (Accessed: 24 October 2022).

Barnett, S. R. (1999) 'The Right to One's Own Image: Publicity and Privacy Rights in the United States and Spain', *The American Journal of Comparative Law,* 47(4), pp. 555–581 [Online]. Available at: https://doi.org/10.2307/841069 (Accessed: 26 October 2022).

Beling, E. (1928) *Deutsches Reichsstrafprozessrecht*. Berlin: W. de Gruyter & Co; https://doi.org/10.1515/9783111533315.

Bennecke, H., Beling, E. (1900) *Lehrbuch des deutschen Reichsstrafprozessrechts*. Berlin: Schletter'sche Buchhandlung.

Bieńkowska, B. (1994) *O przedmiocie procesu karnego (na tle zasady kontradyktoryjności)*. Państwo i Prawo.

Birkmeyer, K. (1898) *Deutsches Strafprozessrecht*. Berlin: H. W. Müller.

Borowicz, J. (2001) 'Obowiązek prowadzenia przez pracodawcę dokumentacji osobowej i organizacyjnej z zakresu ochrony danych osobowych', *Praca i Zabezpieczenie Społeczne,* 2001/3, pp. 2–11.

Choudhry, S. (2014) 'Article 7 – Right to Respect for Private and Family Life (Family Life Aspects)' in Peers, S., Hervey, T., Kenner, J., Ward, A. (eds.) *The EU Charter of Fundamental Rights: A Commentary*. 1st edn. London: Hart Publishing, pp. 183–223; https://doi.org/10.5771/9783845259055_226.

Cieślak M. (1959) 'O pojęciu przedmiotu procesu karnego i w sprawie tzw. „podstawy procesu"', *Państwo i Prawo*, 1959/8-9, pp. 333–341.

Clough, J. (2010) *Principles of cybercrime*. New York: Cambridge University Press; https://doi.org/10.1017/CBO9780511845123.

Czopek, J. (2016) 'Bezpieczeństwo i ochrona prywatności młodzieży w Internecie w kontekście edukacji medialnej', *Zeszyty Naukowe Wyższej Szkoły Humanitas. Pedagogika,* 2016/12, pp. 67–73.

Daszkiewicz, W. (1985) *Proces karny: część ogólna*. Toruń: Wydawnictwo Uniwersytetu Mikołaja Kopernika.

De Pietro, C., Francetic, I. (2018) 'E-health in Switzerland: The laborious adoption of the federal law on electronic health records (EHR) and health information exchange (HIE) networks', *Health Policy*, 122(2), pp. 69–74 [Online]. Available at: https://doi.org/10.1016/j.healthpol.2017.11.005 (Accessed: 26 October 2022).

Diggelmann, O., Cleis, M. N. (2014) 'How the right to privacy became a human right', *Human Rights Law Review*, 14(3), pp. 441–458 [Online]. Available at: https://doi.org/10.1093/hrlr/ngu014 (Accessed: 26 October 2022).

Dobrzeniecki, K. (2004) *Prawo a etos cyberprzestrzeni*. Toruń: Wydawnictwo Adam Marszałek.

Drozd, A. (2004) 'Ochrona danych osobowych pracownika (kandydata) po nowelizacji kodeksu pracy', *Praca i Zabezpieczenie Społeczne*, 2004/1, pp. 25–31.

Działocha, K., Zalasiński, T. (2006) 'Zasada prawidłowej legislacji jako podstawa kontroli konstytucyjności prawa', *Przegląd Legislacyjny*, 2006/3, pp. 5–20.

Elenko, E., Underwood, L., Zohar, D. (2015) 'Defining digital medicine', *Nature Biotechnology*, 33(5), pp. 456–461 [Online]. Available at: https://doi.org/10.1038/nbt.3222 (Accessed: 26 October 2022).

Emiliou, N. (1996) *The Principle of Proportionality in European Law: A Comparative Study*. London: Kluwer Law International; https://doi.org/10.1017/S0020589300060346.

Długosz, J. (2017) 'The Principle of Proportionality in European Union Law as a Prerequisite for Penalization', *Adam Mickiewicz University Law Review*, 2017(7), pp. 283–300 [Online]. Available at: https://doi.org/10.14746/ppuam.2017.7.17 (Accessed: 26 October 2022).

Ferens, A. (2021) 'Cyberbezpieczeństwo i cyberryzyko w raportach zintegrowanych i sprawozdaniach zarządu operatorów usług kluczowych', *Zeszyty Teoretyczne Rachunkowości*, 45(2), pp. 31–50 [Online]. Available at: https://doi.org/10.5604/01.3001.0014.9558 (Accessed: 26 October 2022).

Florczak-Wątor, M. (2019) 'Commentary on Art. 61 of the Polish Constitution' in Tuleja, P. (ed.) *Konstytucja Rzeczypospolitej Polskiej. Komentarz.* 1st edn. Warsaw: Wolters Kluwer, pp. 207–210.

Gao, X., Lin, L., Lan, T., Gan, X. (2019) 'Design and Research on the Chinese Medicine Health Management System Based on the Wireless Sensor Network' in Xu, Z., Choo, K. K., Dehghantanha, A., Parizi, R., Hammoudeh, M. (eds.) *Cyber Security Intelligence and Analytics. CSIA 2019. Advances in Intelligent Systems and Computing.* 1st edn. Cham: Springer, pp. 55–56; https://doi.org/10.1007/978-3-030-15235-2_9.

Gekiere, W., Baeten, R., Palm, W. (2010) 'Free movement of services in the EU and health care' in Mossialos, E., Permanand, G., Baeten, R., Hervey, T. K. (eds.) *Health Systems Governance in Europe. The Role of European Union Law and Policy.* 1st edn. Cambridge: Cambridge University Press (Health Economics, Policy and Management), pp. 461–508; https://doi.org/10.1017/CBO9780511750496.012.

Gersdorf, M. (2005) 'Kilka uwag praktycznych o ochronie danych osobowych pracownika', *Praca i Zabezpieczenie Społeczne,* 2005/8, pp. 14–19.

Gibson, W. (2009) *Neuromancer*. Katowice: Wydawnictwo Książnica.

Golec, S. (2018) *Zasada proporcjonalności jako podstawa rozstrzygnięcia sadu administracyjnego w sprawach podatkowych*. Białystok: Uniwersytet w Białymstoku.

Graff, M. (2008) 'Law and finance: Common law and civil law countries compared – An empirical critique', *Economica* 75(297), pp. 60–83.

HANCOCK, B. (2000) 'US and Europe Cybercrime Agreement Problems', *Computers & Security*, 19(4), pp. 306–307 [Online]. Available at: https://doi.org/10.1016/S0167-4048(00)04012-8 (Accessed: 26 October 2022).

HIJMANS, H. (2016) 'Privacy and Data Protection as Values of the EU That Matter, Also in the Information Society' in HIJMANS, H. (ed.) *The European Union as Guardian of Internet Privacy, Law, Governance and Technology Series*. 1st edn. Cham: Springer, pp. 17–75; https://doi.org/10.1007/978-3-319-34090-6_2.

HOLTZ-BACHA, C. (2004) 'Germany: How the private life of politicians got into the media', *Parliamentary Affairs*, 57(1), pp. 41–52 [Online]. Available at: https://doi.org/10.1093/pa/gsh004 (Accessed: 26 October 2022).

HUCAŁ, M. (2017) 'Ochrona danych osobowych w związkach wyznaniowych w świetle unijnego rozporządzenia nr 2016/679', *Studia z Prawa Wyznaniowego,* 2017(20), pp. 185–222 [Online]. Available at: https://doi.org/10.31743/spw.264 (Accessed: 26 October 2022).

IZYUMENKO, E. (2016) 'The freedom of expression contours of copyright in the digital era: a European perspective', *The Journal of World Intellectual Property*, 19(3–4), pp. 115–130 [Online]. Available at: https://doi.org/10.1111/jwip.12057 (Accessed: 26 October 2022).

JACOBS, F. G. (1999) 'Recent Developments in the Principle of Proportionality in European Community Law', in ELLLIS, E. (ed.) *The Principle of Proportionality in the Laws of Europe*. 1st edn. Oxford: Bloomsbury Publishing, pp. 1–23.

JANKOWSKA, M. (2015) 'Podmiotowość prawna sztucznej inteligencji?' in BIELSKA-BRODZIAK, A. (ed.) *O czym mówią prawnicy mówiąc*. 1st edn. Katowice: Wydawnictwo Uniwersytetu Śląskiego, pp. 171–197.

JANOWSKI, J. (2012) 'Cybernetyzacja prawa' in GALEWSKA, E., KOTECKA, S. (ed.) *X-lecie CBKE. Księga pamiątkowa z okazji 10-lecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego*. 1st edn. Warsaw: Wydawnictwo Oficyna Prawnicza, pp. 394–409.

JĘDRUSZCZAK, K. (2005) 'Prywatność jako potrzeba w ramach koncepcji siebie', *Roczniki Psychologiczne*, 8(2), pp. 111–135.

JOSEPH S., CASTAN, M. (2013) *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary*. Oxford: Oxford University Press; https://doi.org/10.1093/law/9780199641949.001.0001.

KASZUBA, P. (2020) 'Niebezpieczeństwa wirtualizacji życia i wartości w cyberprzestrzeni', *Studia Socialia Cracoviensia,* 12(1), pp. 49–72.

KIEL, J. M. (2001) *Information Technology for the Practicing Physician*. New York: Springer; https://doi.org/10.1007/b97660.

KORENICA, F. (2015) *The EU Accession to the ECHR, Between Luxembourg's Search for Autonomy and Strasbourg's Credibility on Human Rights Protection*. Cham: Springer; https://doi.org/10.1007/978-3-319-21759-8.

KRĘCISZ-SARNA, A. (2018) 'Ochrona danych osobowych w ogólnym postępowaniu administracyjnym', *Roczniki Administracji i Prawa*, 18(2), pp. 199–213 [Online]. Available at: https://doi.org/10.5604/01.3001.0013.1791 (Accessed at: 26 October 2022).

KUCZYŃSKI, G. (2009) 'Ochrona prywatności w internecie', *Marketing w praktyce,* 2009/3, pp. 30–32.

LINKOUS, J. D. (2001) *A Rapidly Evolving Definition of Telemedicine* in KIEL, J. M. (ed.) *Information Technology for the Practicing Physician*. New York: Springer, p. 226; https://doi.org/10.1007/0-387-21857-2_26.

MADSEN, W. (1992) *International, National and Sub-National Data Protection Laws*. London: Springer; https://doi.org/10.1007/978-1-349-12806-8.

Marczyk, M. (2018) 'Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru', *Przegląd Teleinformatyczny*, 6(24), pp. 59–72 [Online]. Available at: https://doi.org/10.5604/01.3001.0012.7212 (Accessed: 26 October 2022).

Marmor, A. (2015) 'What is the right to privacy?', *Philosophy & Public Affairs*, 43(1), pp. 3–26 [Online]. Available at: https://doi.org/10.1111/papa.12040 (Accessed: 26 October 2022).

McCloskey, H. J. (1980) 'Privacy and the right to privacy', *Philosophy,* 55(211), pp. 17–38 [Online]. Available at: https://doi.org/10.1017/S0031819100063725 (Accessed: 26 October 2022).

McGregor, L. (2015) 'Alternative dispute resolution and human rights: developing a rights-based approach through the ECHR', *European Journal of International Law,* 26(3), pp. 607–634 [Online]. Available at: https://doi.org/10.1093/ejil/chv039 (Accessed: 27 October 2022).

McKay, R. B. (1965) 'The Right of Privacy: Emanations and Intimations', *Michigan Law Review,* 64(2), pp. 259–282 [Online]. Available at: https://doi.org/10.2307/1287069 (Accessed: 27 October 2022).

McQuade, S. D. (2008) *Encyclopedia of Cybercrime*. London: Greenwood Press.

Mendoza, I., Bygrave, L. A. (2017) 'The right not to be subject to automated decisions based on profiling' in Synodinou, T.E., Jougleux, P., Markou, C., Prastitou, T. (eds.) *EU Internet Law: Regulation and Enforcement*. 1st edn. Cham: Springer, pp. 77–98; https://doi.org/10.1007/978-3-319-64955-9_4.

Mezglewski, A. (2007) 'Działalność związków wyznaniowych a ochrona danych osobowych', *Studia z Prawa Wyznaniowego*, 2007/10, pp. 5–21.

Michalak, A. (2016) 'Dostęp do informacji publicznej a ochrona prywatności na tle aktualnego orzecznictwa sądów administracyjnych', *Przegląd Sejmowy*, 2016/2, pp. 47–65.

Michałowska, K. (2013) 'Prawo do życia rodzinnego na tle ogólnie pojmowanej prywatności jednostki', *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie,* 2013(911), pp. 51–64.

Mider, D., Ziemak, E. A. (2021) 'Technologie wspierające prywatność – ideologia, prawo, wdrożenia', *Przegląd Bezpieczeństwa Wewnętrznego*, 24(13), pp. 132–172 [Online]. Available at: https://doi.org/10.4467/20801335PBW.21.003.13560 (Accessed: 27 October 2022).

Milanović, M., Papić, T. (2018) 'The applicability of the ECHR in contested territories', *International & Comparative Law Quarterly,* 67(4), pp. 779–800 [Online]. Available at: https://doi.org/10.1017/S0020589318000234 (Accessed: 27 October 2022).

Miller, M. (2014) *The Ultimate Guide to bitcoin*. Indianapolis: Pearson Education.

Nakanishi, Y. (2018) 'Mechanisms to Protect Human Rights in the EU's External Relations' in Nakanishi, Y. (ed.) *Contemporary Issues in Human Rights Law*. 1st edn. Singapore: Springer, pp. 3–21; https://doi.org/10.1007/978-981-10-6129-5_1.

Niczyporuk, J. (1999) 'Administracja ochrony danych osobowych', *Zeszyty Naukowe/Wyższa Szkoła Informatyki i Zarządzania,* 1, pp. 29–35.

Niklas, J. (2014) 'Prywatność w internecie', *Infos zagadnienia społeczno-gospodarcze,* 13(173), pp. 1–4.

Ning, H., Ye, X., Bouras, M. A., Wei, D., Daneshmand, M. (2018) 'General cyberspace: Cyberspace and Cyber-Enabled Spaces', *IEEE Internet of Things Journal,* 5(3), pp. 1843–1856 [Online]. Available at: https://doi.org/10.1109/JIOT.2018.2815535 (Accessed: 27 October 2022).

Nowacki, J. (1995) *Rządy prawa: Dwa problemy*. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

NOWAK, A. (2013) 'Cyberprzestrzeń jako nowa jakość zagrożeń', *Zeszyty Naukowe Akademii Obrony Narodowej*, 3(92), pp. 5–46 [Online]. Available at: https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-9a6e86fb-86d1-4879-b31d-bb555819fccb (Accessed: 27 October 2022).

NOWICKI, M. (2013) *Wokół Konwencji Europejskiej: Komentarz do Europejskiej Konwencji Praw Człowieka*. Warsaw: Wolters Kluwer.

O'BRIEN, D. (1902) 'The Right of Privacy', *Columbia Law Review*, 2(7), pp. 437–448 [Online]. Available at: https://doi.org/10.2307/1109924 (Accessed: 27 October 2022).

OHLY, A. (2018) 'The broad concept of „communication to the public" in recent CJEU judgments and the liability of intermediaries: primary, secondary or unitary liability?', *Journal of Intellectual Property Law & Practice*, 13(8), pp. 664–675 [Online]. Available at: https://doi.org/10.1093/jiplp/jpy083 (Accessed: 27 October 2022).

ORĘZIAK, B. (2019) *Cyberprzestępczość w aspektach proceduralnych: dowody elektroniczne a nowoczesne formy przestępczości.* Warsaw: Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie.

PIECHOTA, M. (2012) 'Konstytucyjne prawo do ochrony zdrowia jako prawo socjalne i prawo podstawowe*', Roczniki Administracji i Prawa,* 12, pp. 93–104 [Online]. Available at: http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-f268c2a7-865e-4791-884e-45cf2e364fc2 (Accessed: 27 October 2022).

PIKUL, K. (2012) 'Materialne przesłanki przeszukania w kpk', *Nowa kodyfikacja prawa karnego,* 2012(28), pp. 161–170.

POPIOŁEK, M., WIECZORKOWSKI, J. (2018) 'Prywatność a użytkowanie technologii informacyjno-komunikacyjnych–przegląd badań', *Ekonomiczne Problemy Usług,* 131(1), pp. 261–270 [Online]. Available at: https://doi.org/10.18276/epu.2018.131/1-26 (Accessed: 27 October 2022).

REHOF, L. (1999) 'Article 12' in ALFREDSSON, G. S., EIDE, A. (eds.) *The Universal Declaration of Human Rights: A Common Standard of Achievement*. 1st edn. The Hague, Boston: Martinus Nijhoff Publishers, pp. 251–265.

ROJSZCZAK, M. (2019) 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace', *Information & Communications Technology Law,* 29(1), pp. 22–44 [Online]. Available at: https://doi.org/10.1080/13600834.2020.1705033 (Accessed: 27 October 2022).

ROSENFELD, E. H. (1909) *Der Reich-Strafprozess*. Berlin: J. Guttentag; https://doi.org/10.1515/9783112386002.

RUBENFELD, J. (1989) 'The right of privacy', *Harvard Law Review*, 102(4), pp. 737–807 [Online]. Available at: https://doi.org/10.2307/1341305 (Accessed: 27 October 2022).

SAUER, W. (1951) *Allgemeine Prozessrechtslehre*. Berlin, Heidelberg: Springer.

SCHAFF, L. (1959) 'Wszczęcie postępowania karnego a problematyka podstawy i przedmiotu procesu', *Państwo i Prawo*, 1959/2, pp. 255–260.

SCHMIDT, E. (1952) *Lehrkommentar zur StPO und zum GVG Teil I: Die rechts theoretischen und die rechtspolitischen Grundlagen des Strafverfahrensrechts*. Göttingen.

SEZGIN, E. (2018) 'Introduction to Current and Emerging mHealth Technologies: Adoption, Implementation, and Use' in SEZGIN, E., YILDIRIM, S., ÖZKAN-YILDIRIM, S., SUMUER, E. (eds.) *Current and Emerging mHealth Technologies: Adoption, Implementation, and Use*. 1st edn. Cham: Springer, pp. 1–6; https://doi.org/10.1007/978-3-319-73135-3_1.

SHAPIRO, A. (1999) 'The Internet', *Foreign Policy*, 1999(115), pp. 14–27 [Online]. Available at: https://doi.org/10.2307/1149490 (Accessed: 27 October 2022).

SIBIGA, G. (2003) 'Dostęp do informacji publicznej a prawa do prywatności jednostki i ochrony jej danych osobowych', *Samorząd Terytorialny,* 2003/11, pp. 5–11.

SIENKIEWICZ, P. (2009) 'Terroryzm w cybernetycznej przestrzeni' in JEMIOŁA, T., KIESIELNICKI, J., RAJCHEL, K. (eds.) *Cyberterroryzm – nowe wyzwania XXI wieku.* 1st edn. Warsaw: Wyższa Szkoła Informatyki, Zarządzania i Administracji, pp. 194–200.

SIEROŃ, A. (2013) 'Czym jest Bitcoin', *Wrocław Economic Review*, 19(4), pp. 31–51 [Online]. Available at: https://wuwr.pl/ekon/article/view/8379/7997 (Accessed: 27 October 2022).

SKOCZYLAS, D. (2018) 'Przetwarzanie danych osobowych a prawo do bycia zapomnianym i prawo do przenoszenia danych na gruncie RODO', *Acta Iuris Stetinensis,* 24(4), pp. 87–100 [Online]. Available at: https://doi.org/10.18276/ais.2018.24-04 (Accessed: 27 October 2022).

SNOPKIEWICZ, K. (2020) 'Przegląd zagrożeń w cyberprzestrzeni'*, Studia Administracji i Bezpieczeństwa,* 1(9), pp. 29–41 [Online]. Available at: https://bibliotekanauki.pl/articles/1877221 (Accessed: 27 October 2022).

SOBCZYK, P. (2017) 'Ochrona danych osobowych jako element prawa do prywatności', *Zeszyty Prawnicze,* 9(1), pp. 299–318 [Online]. Available at: https://doi.org/10.21697/zp.2009.9.1.14 (Accessed: 27 October 2022).

SPEED, J. G. (1896) 'The right of privacy', *The North American Review,* 163(476), pp. 64–74 [Online]. Available at: http://www.jstor.org/stable/25118676 (Accessed: 27 October 2022).

ŚWIERCZYŃSKI, M., ŻARNOWIEC, Ł. (2019) 'Prawo właściwe dla odpowiedzialności za szkodę spowodowaną przez wypadki drogowe z udziałem autonomicznych pojazdów', *Zeszyty Prawnicze,* 19(2), pp. 101–135 [Online]. Available at: https://doi.org/10.21697/zp.2019.19.2.03 (Accessed: 27 October 2022).

TADEUSIEWICZ, R. (2007) 'Wychowywanie dla cyberprzestrzeni jednym z warunków zapobiegania cyberuzależnieniom' in MASTALERZ, E., PYTEL, K., NOGA, H. (eds.) *Cyberuzależnienia@: przeciwdziałanie uzależnieniom od komputera i Internetu*. 1st edn. Kraków: Niezależne Zrzeszenie Studentów Akademii Pedagogicznej, pp. 23–30.

THOMSON, J. J. (1975) 'The right to privacy'*, Philosophy & Public Affairs*, pp. 295–314.

TOKARCZYK, R. (2008) *Komparatystyka prawnicza*. Warsaw: Wolters Kluwer.

TROUILLE, H. (2000) 'Private life and public image: Privacy legislation in France', *International & Comparative Law Quarterly,* 49(1), pp. 199–208 [Online]. Available at: https://doi.org/10.1017/S0020589300064034 (Accessed: 27 October 2022).

VAN DEN HAAG, E. (2017) 'On privacy' in PENNOCK, J.R., CHAPMAN, J.W. (eds.) *Privacy & Personality.* 1st edn. New York: Routledge, pp. 149–168; https://doi.org/10.4324/9781315127439-8.

VAN DER SLOOT, B. (2017) 'Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected Under Article 8 ECHR' in TAYLOR, L., FLORIDI, L., VAN DER SLOOT, B. (eds.) *Group Privacy. Philosophical Studies Series*. 1st edn. Cham: Springer, pp. 197–224; https://doi.org/10.1007/978-3-319-46608-8_11.

VESTED-HANSEN, J. (2014) 'Article 7 – Respect for Private and Family Life (Private Life, Home and Communications)' in PEERS, S., HERVEY, T., KENNER, J., WARD, A. (eds.) *The EU Charter of Fundamental Rights: A Commentary.* 1st edn. Baden-Baden: Nomos, pp. 196–225; https://doi.org/10.5771/9783845259055_196.

VON KRIES, A. (1892) *Lehrbuch des deutschen Strafprozessrechtes*. Freiburg: Verlagsbuchhandlung von Mohr.

WACHTER, S. (2018) 'Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR', *Computer Law & Security Review,* 34(3), pp. 436–449 [Online]. Available at: https://doi.org/10.1016/j.clsr.2018.02.002 (Accessed: 27 October 2022).

WANG, X., LOVE, P.E.D., KIM, M. J., WANG, W. (2014) 'Mutual awareness in collaborative design: An Augmented Reality integrated telepresence system', *Computers in Industry*, 65(2), pp. 314–324 [Online]. Available at: https://doi.org/10.1016/j.compind.2013.11.012 (Accessed: 27 October 2022).

WEINREB, L. L. (2000) 'The Right to Privacy', *Social Philosophy and Policy,* 17(2), pp. 25–44 [Online]. Available at: https://doi.org/10.1017/S0265052500002090 (Accessed: 27 October 2022).

WIBLE, B. (2003) 'A Site Where Hackers are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime', *The Yale Law Journal*, 112(6), pp. 1577–1623 [Online]. Available at: https://doi.org/10.2307/3657453 (Accessed: 27 October 2022).

WIEL, S. C. (1918) 'Origin and Comparative Development of the Law of Watercourses in the Common Law and in the Civil Law', *California Law Review*, 6(4), pp. 245–267 [Online]. Available at: https://doi.org/10.2307/3474107 (Accessed: 27 October 2022).

WIEWIÓROWSKI, W. R. (2014) 'Ochrona prywatności jako ograniczenie prawa do ponownego przetwarzania informacji publicznej'*, Gdańskie Studia Prawnicze,* 2014(31), pp. 145–155.

WOJCIESZAK, A. (2021) 'O poszanowaniu godności człowieka na przykładzie polskich gwarancji jej ochrony oraz orzecznictwa Sądu Najwyższego Stanów Zjednoczonych Ameryki', *Studia Iuridica Lublinensia*, 30(5), pp. 701–720; https://doi.org/10.17951/sil.2021.30.5.701-721.

WÓJTOWICZ, A., CELLARY, W. (2018) 'New challenges for user privacy in cyberspace', in MOALLEM, A. (ed.) *Human-Computer Interaction and Cybersecurity Handbook*. 1st edn. Boca Raton: CRC Press, pp. 77–96; https://doi.org/10.1201/b22142-4.

WRONKOWSKA, S. (2006) 'Zasady przyzwoitej legislacji w orzecznictwie Trybunału Konstytucyjnego' in ZUBIK, M. (ed.) *Księga XX-lecia orzecznictwa Trybunału Konstytucyjnego*. 1st edn. Warsawa, pp. 671–689.

ZALESKI, Z. (1998) 'Prawo do prywatności. Spojrzenie psychologiczne', *Czasopismo Psychologiczne*, 4(4), pp. 218–238.

ZDZIKOT, T. (2022) 'Cyberspace and Cybersecurity', in CHAŁUBIŃSKA-JENTKIEWICZ, K. RADONIEWICZ, F., ZIELIŃSKI, T. (eds.) *Cybersecurity in Poland*. 1st edn. Cham: Springer, pp. 9–21; https://doi.org/10.1007/978-3-030-78551-2_2.

ZIELIŃSKI, A. (2021) 'Konstytucyjność art. 3 ust. 6 ustawy o Rzeczniku Praw Obywatelskich', *Państwa i Prawa*, 2021/7, p. 23.

ZUBIK, M. (2008) *Selection of international law documents concerning human rights*. Warsaw.

## Other titles in the book series
## *Studies of the Central European Professors' Network*

**2021**

Tímea Barzó, Barnabás Lenkovics (eds.): *Family Protection From a Legal Perspective*

Zoltán J. Tóth (ed.): *Constitutional Reasoning and Constitutional Interpretation*

Paweł Sobczyk (ed.): *Religious Symbols in the Public Sphere*

Marcin Wielec (ed.): *The Impact of Digital Platforms and Social Media on the Freedom of Expression and Pluralism*

**2022**

János Ede Szilágyi (ed.): *Constitutional Protection of the Environment and Future Generations: Legislation and Practice in Certain Central European Countries*

Paweł Sobczyk (ed.): *Content of the Right to Parental Responsibility: Experiences – Analyses – Postulates*

Zoltán J. Tóth (ed.): *Constitutional and Legal Protection of State and National Symbols in Central Europe*

**Design, layout**
IDEA PLUS (Elemér Könczey, Botond Fazakas)
Kolozsvár / Cluj-Napoca (Romania)

**Printed and bound by**
AK NYOMDA
Martonvásár (Hungary)