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.