Chapter V

The Right to Privacy in the Digital Age from the Viewpoint of the Slovak Legal Order

Katarína Šmigová

1. Introduction

Privacy *per se*, according to the Oxford Dictionary, is generally understood as a state in which one is not observed or disturbed by other people; even more, it is considered to be the state of being free from public attention.[1] Keeping in mind the digital aspects of today society, it is challenging that the definition has not been changed yet, especially in relation to the observance part or to the public attention part since it is greatly present in the current discussion about protection of the right to privacy. It is one of the defining elements of today's world. In our information society, one's personal data is its integral part. There is information all around us—not only about the world but about ourselves as well. And if it is in an electronic form that is preferred today, it can be spread worldwide quicker than ever before.

It has been a part of the human rights law ever since human rights are afforded to individuals regardless of his or her approval; their guarantee depends only on the fact of a dignity of a human being, and the foundation of freedom, justice, and peace.[2] Such an understanding of the whole area of human rights protection

1 *Oxford Dictionary.* https://languages.oup.com/google-dictionary-en/.

2 See Preamble of the Universal Declaration of Human Rights, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948).

Katarína Šmigová (2023) The Right to Privacy in the Digital Age from the Viewpoint of the Slovak Legal Order. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 165–197. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_5

includes the concept of those rights being inviolable and irrevocable (no one can be deprived of these rights), inalienable (they cannot be transferred to another), imprescriptible (and therefore their duration is indefinite), and indefeasible (they exist independently of the will of the legislature who can recognize them but cannot cancel them).[3]

Despite different sources' claim of origin,[4] human rights are not only ethical or moral principles since their recognition and effective protection are one of the principles of democracy and the rule of law.[5] It is important to remember this understanding while analyzing the way most people enter the digital world, since they usually just tick to agree with terms and conditions.[6] Although they have the right to self-determination,[7] especially today, the digital world has created a virtual reality that is not only preferred in some cases but also automatically entered into without checking to see how one's information will be used. Right of an individual to informational self-determination is a right closely related to the right to privacy. It has been deeply examined in relation with the GDPR, which requires data processing in good faith and transparency only for specified, explicit, and legitimate purposes and only for the necessary time.[8] These are rules that are to be respected from companies processing personal data; however, in case an individual ticks automatically his or her consent without reading terms and conditions, it is difficult to require the real goal of the regulation under all circumstances.[9]

Although there is no particular case law of the supreme courts of the Slovak Republic in relation to the informed consent, relevant international or supranational legal acts might be helpful.[10]

3 See Art. 12 of the Constitution of the Slovak Republic, Act no. 460/1992 Coll.

4 Vršanský and Valuch, 2016, p. 200.

5 See Preamble of the European Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe Treaty Series 005, Council of Europe, 1950.

6 See Sandle, 2020. https://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127.

7 Right to self-determination in the context of this chapter is not considered to be a right to self-determination according to Art. 1 of the International Covenant on Civil or Political Rights or Art. 1 of the International Covenant on Economic, Social and Cultural Rights, but right of an individual to informational self-determination.

8 For more detailed information see the Regulation itself: *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

9 GDPR is not the first set of legal norms that aim at protection of data processing, see e.g., The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

10 Keeping in mind that the informed consent has been analyzed mostly in relation to the medical care, the GDPR application in relation to a valid consent to process personal data has been chosen since it has been elaborated more in relation to the digital world, it is so also in the academic sphere. See e.g., https://dl.acm.org/doi/pdf/10.1145/3319535.3354212.

Consent that is required today to gain access to most social media might be considered in opposition to truly valid consent according to the GDPR.[11] Although it might be given in a good faith, there are several conditions that are to be met.[12] However, they are usually fulfilled only in a theory by checking a box to agree to terms and conditions. Individuals usually know that they must be given a free choice, i.e., they must be able to refuse or withdraw their consent without being at a disadvantage. Nevertheless, in automatic acceptance, people do not check whether the organization asking for a consent requires consent to the processing of unnecessary personal data—data that is not necessary to provide searched service. Moreover, who checks not only the identity of the organization processing data, their type, and purposes for which they are being processed—and how often those checks occur—as well as whether there is the possibility of withdrawing the given consent. The data might be used also for profiling and even more that the data might be transferred to third countries that are not within GDPR application, e.g., in case that the information concerns political opinion, religion, genetic data, data concerning health, or sex life, if these have been demonstrably disclosed by the person concerned.

If one considers adoption of the GDPR as another step of privacy protection after the well-known Google case,[13] i.e., the right to be forgotten, it might still have limits. The most important limit is the one that concerns jurisdiction. There is no doubt that state jurisdiction, which is based on the territorial nature of the state respecting the physical boundaries of the country's geography, might be considered distant from the concept of digital world, the virtual nature of which is primarily based on crossing borders; for some authors, even the issue of boundlessness is included.[14] Nevertheless, it should be pointed out that both of these concepts incorporate an aspect of control; in both cases, therefore, a state must be present in relation to its jurisdiction to create and enforce law, by judicial tools if necessary.[15]

To respect the academic goal of the present project of the Central European Academy, the present chapter is not so far reaching as to analyze and offer solutions to guarantee proper application and support of the right to privacy in the digital era. The challenges of the proper use of technological conveniences and their impact in relation to an individual and his or her right to privacy far exceed the scope of this chapter. Nevertheless, this contribution aims to analyze selected aspects of the right to privacy protection in the Slovak Republic. The overall approach is taken from the constitutional point of view, since the Constitution is the fundamental law of a state. First, the term of privacy and its content and challenges of this traditional concept in terms of the digital world is analyzed; accordingly, the text of the Constitution of the

11 See Art. 5 of the GDPR.

12 See e.g., Guidelines on Consent under Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/623051.

13 Court of Justice of the European Union (Grand Chamber), Case C-131/12, Google Spain SL v Agencia Española de Protección de Datos, 13 May 2014.

14 Barlow, 1996, https://www.eff.org/cyberspace-independence.

15 Brownlie, 2013, pp. 325 et seq.

Slovak Republic and the case law of the Constitutional Court of the Slovak Republic within the determined research area is studied. The focus is given not only on the term of privacy but also on all the issues that are covered by this term in several constitutional articles, especially the right to personal honor and reputation, name protection, protection of private and family life, protection of personal data, domestic freedom, or protection of personal communication. The question is whether this framework of the constitutional protection of the right to privacy is applicable also in the case of digital age or there is something that must be improved or changed so that the protection of this right is effective. While focusing on the Constitution, other relevant provisions of selected law are examined. The selection has been taken based on the most important challenges in relation to the right to privacy within Slovak legal order and the most important achievements; existence of relevant international case law has been another important selection factor. To mention some examples, the Slovak Civil Code providing legal tools to protect the right to privacy in case of its violation is emphasized separately. Moreover, Criminal Code, Labor Code, Act on Personal Data Protection, and Act on Electronic Communications have been taken under closer scrutiny. Since the GDPR has already been profoundly analyzed because of its specific status and purpose,[16] only some of its aspects are included into this chapter as has been done e.g., in relation to a valid consent. Finally, some groups of individuals have been selected, to name employees or children as least, since these individuals prove to be vulnerable and their status has become a challenge for proper privacy protection.

To set the hypothesis of the chapter, case law and especially legislation in the Slovak Republic is reactive in the sense that it does not actively propose new solutions to challenges of the digital world, but merely applies existing tools whenever and wherever applicable. It is not a reproof—merely reflection upon the current situation, since the technical development in relation to a digital world is so intense and rapidly changing that it has many times meant that the corresponding response of the legislature is either too slow or waiting for solutions from other sources, i.e., international or supranational inspiration. Moreover, it is difficult to react when sometimes even those whose right to privacy has been violated do not know about this violation, especially when he or she has given their consent freely to interlink or even open their privacy to the digital world.

16 To specify, the regulation is directly applicable in all the EU Member States; the aim of the present research, quite opposite, is to analyze specific features of the Slovak legal framework. It is therefore enough to point out that the regulation has been adopted to answer challenges personal data protection within the digital world. The biggest change lies in its purpose to protect the personal data of European Union citizens' and residents' data, regardless of their location and where they have their registered office or server. The concept of territoriality has thus been replaced by the concept of personality, the decisive factor is the person whose data is being processed and not the location of the data itself. However, Art. 9, para. 2 e) of this regulation is important since it indicates that the ban on processing personal data does not apply in relation to specific categories of personal data, e.g., political opinion, religion genetic data, data concerning health, sex life, if these have been demonstrably disclosed by the person concerned. For more information concerning the situation in Slovakia, see e.g., Garayová, 2020.

2. Term of privacy within Art. 16 of the Constitution of the Slovak Republic

Neither the right to privacy nor privacy as such is defined in the Slovak constitutional framework.[17] Nevertheless, the Constitution guarantees in its Art. 16 the right of every individual to integrity and privacy. As for limitations of this right, it may be restricted only in cases specifically provided by a law.[18] So far, it is not very much different from any other national or international legal order. Nevertheless, it is rather rare that such a provision is a part of the same article as the prohibition of torture.[19] Such a systematic classification has obviously also become a challenge in relation to the interpretation of Art. 16 of the Constitution. However, the Court has explained that the constitutional protection of the right of privacy is connected with inviolability of a person, therefore privacy is associated with body integrity and material values of private nature.[20] It is true that Art. 16 of the Convention is within articles protecting physical integrity; nevertheless, the Court shares the opinion of European Court of Human Rights emphasizing that the concept of "private life" is a broad concept encompassing, *inter alia*, aspects of an individual's physical and social identity, including the right to personal autonomy, personal development, and the establishment and development of relationships with other human beings and the outside world.[21] The protection of private life must be therefore understood in a broader sense than the protection of life from publicity: it also includes the right to establish and develop relationships with other human beings, particularly in the emotional sphere, to develop and fulfill one's own personhood.[22] Art. 8 of the Convention, like Art. 2 of the Convention, implies not only the negative obligation of the state not to interfere with privacy, but also its positive obligation to effectively ensure respect for private life, which is implemented in particular by the adoption of legislation to protect privacy. For the protection of rights to be effective in practice, there must be an effective administrative and judicial apparatus within which the individual can enforce his or her rights, particularly in cases of serious violations of physical integrity of complainants.[23]

Since there is no definition of the right to privacy in the Constitution as such, there have been several attempts to provide an understanding of this right. One of the most quoted definitions is the one of the Supreme Court of the Slovak Republic, which defined it as the right of a person to decide independently, at his or

17 See e.g., Constitutional Court, II. ÚS 424/2012 from November 6, 2014, finding, para. 33.
18 See Art. 16 of the Constitution of the Slovak Republic.
19 See Art. 16, para. 2 of the Constitution of the Slovak Republic: No one shall be subjected to torture or cruel, inhuman, or degrading treatment or punishment.
20 Constitutional Court, II. ÚS 19/97 from May 13, 1997, finding, p. 17.
21 Constitutional Court, II. ÚS 424/2012 from November 6, 2014, finding, para. 34.
22 Ibid.
23 Ibid. para. 35.

her own discretion, whether and to what extent the facts of his or her private life should be disclosed to others or made public.[24] The violation of the right to privacy within this meaning is not only the unauthorized acquisition of information and knowledge about the privacy of a person, but also the unauthorized dissemination of that information and knowledge. The consequence of an unwarranted interference with the right to privacy may be a substantial diminution of dignity or esteem in society, but this consequence is not the only legally required manifestation of the seriousness of the harm caused to the individual.[25] Consequently, procedurally speaking, the individual who has suffered harm does not have an obligation to prove that the unjustified interference has resulted in a reduction in his or her dignity in society.[26]

Originally, the right to privacy concerned exclusively natural person.[27] According to the initial interpretation of the Court, constitutional protection of privacy is associated with inviolability of a person and therefore especially its body integrity is at stake.[28] Moreover, at the beginning of its decision-making activity, the Court explicitly excluded a legal person from being a subject of privacy protection according to Art. 16 of the Constitution.[29] Nevertheless, taking into account decisions of the ECtHR,[30] the case law of the Constitutional Court has reconsidered its interpretation and included legal persons under the protection of Art. 16. Furthermore, even protection to reputation has been originally provided for only natural persons. However, the Court has reconsidered its approach in this area, and has observed that legal persons deserve not only protection under the Civil Code but also under the Constitution.[31]

Moreover, the inviolability of privacy as *lex generalis* in relation to the right to privacy has included not only rights related to physical integrity but also rights protected by other articles of the Constitution. In *Niemietz*, interpretation of private life has influenced the interpretation of the inviolability of the dwelling, which is another right protected by the Constitution, since in some contexts, work may form part of a person's life to such a degree that it becomes impossible to know in what capacity he or she is acting at a given moment of time—a private or a professional one.[32]

As it has been indicated, the inviolability of the right to privacy must be applied not only by negative obligation of a atate not to interfere directly into privacy of

24 Order of the Supreme Court of the Slovak Republic No. 3 Cdo 137/2008 from 18 February 2010, p. 9.
25 Ibid.
26 Order of the Supreme Court of the Slovak Republic No. 3 Cdo 137/2008 from 18 February 2010, p. 9.
27 Constitutional Court, I. ÚS 6/97 from 23 January 1997, decision, p. 3.
28 Compare Constitutional Court, II. ÚS 19/97 from 13 May 1997, finding, p. 17.
29 Constitutional Court, I. ÚS 6/97 from 23 January 1997, decision, p. 3.
30 E.g., ECtHR, *Niemietz v. Germany*, no. 13710/88, 16 December 1992.
31 See Constitutional Court, II. ÚS 456/2018 from 26 September 2018, decision.
32 Compare ECtHR, *Niemietz v. Germany*, no. 13710/88, 16 December 1992, para. 29.

individuals, and if so, only within limits set out by law, but also by positive duties to adopt such a legal framework that fully respects and ensures respect of human rights also within private persons relations.[33] Moreover, in case of a violation, there must be a possibility guaranteed to an individual to have his or her claim of right to privacy violation inquired.

If the text of Art. 16 of the Constitution and Art. 8 of the Convention is compared, it is surprising that the Constitution does not specify legitimate aims based on which interference into the right to privacy might be justified. Since most articles of the Constitution protecting several aspects of the right to privacy miss these legitimate aims, it is understandable that the right to privacy protected by the Constitution is being interpreted as applying conditions specified by the Convention. It is the case of not only legality, since this limitation is included into the text of Art. 16 of the Convention but lacks legitimate aims and the principle of proportionality. It means that although the Convention says nothing in most of the relevant articles protecting the right to privacy in relation to legitimate aims or proportionality, the decision-making activity of the Court strictly observes the jurisprudence of the ECtHR. The material reason is obvious since they both protect the same right. Nevertheless, there is also a formal reason: the position of the Convention in the Slovak legal order. The Convention is an international treaty on human rights and fundamental freedoms that was ratified by the Slovak Republic and promulgated in a manner laid down by law, and as such it is not only a part of the Slovak legal order but also has primacy over the law, since it provides greater scope of constitutional rights and freedoms.[34]

As mentioned earlier, the right to privacy in the constitutional framework of the Slovak Republic is included in the same article as the prohibition of torture, inhuman or degrading treatment, or punishment that has been consistently reviewed in case of personal checks, isolation, and/or monitoring while being in custody. It is rather clear that the right to privacy is violated when the right to personal freedom is violated by unlawful restriction. On the other hand, it is understandable that in case of lawful detention or deprivation of liberty, one cannot argue that one's right to privacy has been violated, since in this case, loss of privacy is an integral part of the process whose goal could not be otherwise achieved.

33 Art. 1 of the European Convention of Human Rights as interpreted in *Marcx v. Belgium*, no. 6833/74, 13 July 1979. But compare *Evans v. UK*, no. 6339/05, 10 April 2007 where the ECtHR did not consider it important to specify whether it decided the case in the context of positive or negative obligations of a State.

34 Compare Art. 154c of the Constitution of the Slovak Republic.

3. Other aspects of the right to privacy protected by Art. 19 of the Constitution and the Civil Code

According to Art. 19 of the Convention, everyone has the right to the preservation of human dignity, personal honor, reputation, and the protection of one's good name. Moreover, everyone has the right to protection against unauthorized collection, publication, or other misuse of personal data. Finally, everyone has the right to protection against unauthorized interference in private and family life. Again, as there is no specific condition to verify the lawfulness of an interference into these rights directly in Art. 19 of the Convention, such an interference could be realized only based on law and to the extent specified by law, to achieve legitimate aims according to the Convention and, according to the Convention, to the extent necessary in a democratic society.

The way how partly complicatedly the right to privacy is protected within constitutional framework of the Slovak Republic is best illustrated by the relationship between Art. 16 covering inviolability of a person and his/her privacy and Art. 19 covering protection of human dignity, personal honor, reputation, private and family life, and personal data. Although it has been repeatedly pointed out by the Court that the Convention does not define the term of privacy and private life, the Court has also stressed several times that human rights and freedoms guaranteed by the Convention are to be interpreted and applied in the spirit of international treaties on human rights and freedoms.[35] Therefore, according to the Court case law, protection of a private life under Art. 19, para. 2 concerns protection of intangible assets of a private nature[36] and protection of privacy under Art. 16, para. 1 concerns body integrity and material values of a private nature.[37] When interpreting these articles of the Convention, the Court has emphasized several times that it has considered the case law of the ECtHR according to which "private life is a broad term encompassing, *inter alia*, aspects of an individual's physical and social identity including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world."[38] Therefore it is a broader term than privacy protected by Art. 16 of the Constitution.

Dignity of a human being is under the Convention understood as both, a value based on natural law and a source for positively guaranteed human rights,[39] and the right of an individual to have it protected. Such a protection is guaranteed by the effective positive approach of a state in relation to creation of legal framework respecting and ensuring respect of human dignity. This legal framework includes

35 See e.g., Constitutional Court, PL. ÚS 5/93 from 18 May 1994, decision, pp. 10 et seq.
36 Constitutional Court, II. ÚS 19/97 from 13 May 1997, finding, p. 18.
37 Constitutional Court, II. ÚS 19/97 from May 13, 1997, finding, p. 17.
38 ECtHR, *Evans v. United Kingdom*, no. 6339/05, April 10, 2007, para. 71.
39 See Art. 12 para. 1, first sentence of the Constitution: People are free and equal in dignity and in rights.

not only public law, such as criminal and administrative law, but also private law, especially civil law.

As it has already been indicated, Art. 19 of the Convention protects several aspects of privacy protection. Nevertheless, as the Court has already pointed out, a distinction must be made among them since all the terms, namely human dignity, personal honor, and a good reputation, mean something else.[40] Dignity protects the very essence of individual humanity from humiliation, thus protecting humanity from being only an object of power. Reputation is the perception of a person in the community, in the society, it is a social component; on the other hand, honor is on the border between social and personal, internal concept.[41]

It must be pointed out that the current understanding of the right to privacy has been influenced by the era of non-freedom.[42] According to the Court, there was no public society and therefore no public space, protection of privacy was in fact reduced to neighborhood conflicts or commune conflicts. Such a civilistic understanding must have been changed because of necessity of individuals to "breathe freely" to develop their personality, together with understanding that there is no constitutional right to be perceived in a public space entirely the way they wish.[43] Therefore, even though protection of privacy by Civil Code is broader since it includes not only protection of honor and reputation, relevant norms of the Civil Code have to be applied and interpreted in accordance with the Constitution.[44]

To explain a specific position of the Civil Code, one must analyze hierarchy of norms in the Slovak legal order. To concretize basic protection provided by the Convention, it is the Civil Code of the Slovak Republic that forms the basis of private law protection of personality rights that are a part of right to privacy, particularly its paragraphs 11–16 that protect immaterial aspects of the right to privacy.[45] According to Art. 11 of the Civil Code, the subject of protection of human personality is, in particular, life and health, civil honor and human dignity, privacy, name, and expressions of a personal nature. Moreover, Art. 12 of the Civil Code also regulates the right to the protection of personal documents, portraits, images and video and audio recordings concerning a natural person or his or her expressions of a personal nature that might be produced or used only with the consent of this person unless produced or used for e.g., official, scientific, or artistic purposes.

The means of judicial protection of an individual's personality are, first, a negative action, i.e., a demand to a court to decide upon refrainment from unjustified interference, second, a restitution action, i.e., a demand to a court to decide upon elimination of the consequences of interference and finally, a satisfactory action, i.e.,

40 Constitutional Court, II. ÚS 191/2015 from March 26, 2015, decision, p. 26.
41 Compare Ibid.
42 Constitutional Court, II. ÚS 647/2014 from September 30, 2014, judgment, p. 32.
43 Ibid.
44 Constitutional Court, II. ÚS 152/08 from 15 December 2009, finding, para. 27.
45 Act 40/1964 Coll. Civil Code.

a demand to a court to decide upon adequate satisfaction.[46] These means of judicial protection may be applied individually or cumulatively. Their cumulative application depends on the purpose, e.g., if the unjustified interference with the personal rights persists and a right to satisfaction has arisen, a negative action with a satisfactory action may be filed.

The condition for providing personality protection is unauthorized interference with his or her personal rights that must be capable of causing harm to a person's character, but existence of harm is not a condition *sine qua non*.[47]

In the context of the protection of personality rights in the media, especially social media, there is a particular clash between two rights: freedom of expression, and protection of personality.[48] It is important to refer to the international instruments by which the Slovak Republic is bound, the interpretation of the protection of personality rights should be carried out in accordance with these treaties and the case law of their courts. Freedom of expression is one of the essential foundations of a democratic society.[49] The richest source of case law on freedom of expression is the jurisprudence of the ECtHR in Art. 10 of the Convention. At the same time, the Court considers the decisions of the ECtHR in its decision-making, and this is expressly stated in its decisions.[50] Given the importance of freedom of expression, the exceptions set out in any legal regulation must be interpreted restrictively, and the necessity of each restriction must be convincingly demonstrated.

In connection with the issue of privacy protection, the Supreme Court of the Slovak Republic stated that "a wide range of manifestations and components of a natural person's private life is also reflected in the possibility of various manifestations of privacy interventions and their consequences on protected personal rights."[51] However, in general terms, as mentioned above, most conflicts concern the conflict between right to privacy and the freedom of speech. Analysis of this conflict deserves a separate contribution to the discussion.[52] If compared, both these basic rights are in general of the same importance and weight. It is therefore not acceptable to decide normatively which one is to be given priority. Although one is preceded by the other in the text of the Constitution, it does not mean that in the Convention, the right is given priority in case of a conflict. According to the Court, such an interpretation could not be accepted since any solution to a conflict of two rights guaranteed by the Constitution depends on specific circumstances of the case.[53] It is therefore up to the

46 Števček et al., 2015, pp. 82–94.
47 Števček et al., 2015, pp. 82–94.
48 Drgonec, 2013, pp. 154 et seq.
49 ECtHR, *Handyside* v. UK, no. 5493/72, 7 December 1976, para. 49.
50 See e.g., Constitutional Court, PL. ÚS 5/93 from 18 May 1994, decision, pp. 10 et seq.
51 Decision of the Supreme Court of the Slovak Republic, no. 3 Cdo 137/2008 from February 18, 2010, p. 9.
52 Within the Central European Academy project, a separate Art. will be written upon this clash between the right to privacy and the freedom of expression.
53 Constitutional Court, III. ÚS 673/2017 from November 7, 2017, decision, para. 23.

courts, when discussing a particular dispute, to determine the need to give priority to one of the protected rights by examining the degree of importance of both in the conflict of existing constitutional values.[54] It actually means that all fundamental rights and freedoms are protected only to the extent that the exercise of one right or freedom does not unduly restrict or deny another's right or freedom.[55]

If the right to privacy is claimed to have been violated, there are several issues that courts consider, such as form and content of the speech or public interest involved in case of publicly known persons, especially politicians.[56]

The right to privacy in case of politicians is a very special case of balancing privacy and public interest. In general, more publicly known the person is, more interference into his or her privacy s/he must endure. On the other hand, one should distinguish between statements of facts and evaluative judgments. As for the former, there is no violation of the right to reputation, and for the latter, opinions must meet criteria of materiality, specificity, and proportionality.[57] Especially the issue of proportionality might be at stake since even opinions within realization of the freedom of speech might have limits although persons active in public life are expected to accept critical comments more than ordinary people. As it has already been pointed out, there are limits to the freedom of speech, in the case of public persons, e.g., in relation to attacks that are aimed to influence them in the performance of their duties and to damage public confidence in them and in the office they hold.[58] Moreover, even their personal security must be considered if freedom of speech is realized in a manner that could threaten it.[59]

One of the first issues that reflect a right to privacy of every individual is the right to a name. As for the constitutional right to a name protection under Art. 19, para. 1 of the Constitution, this is elaborated in the provisions of Art. 11 of the Civil Code. According to the Court, the cited provision includes civil honor and human dignity, in addition to the protection of his/her name and expressions of a personal nature.[60] The right to name protection under the provisions of Art. 11 of the Civil Code does not differ in principle from the constitutional right to a name protection under Art. 19, para. 1 of the Constitution. The content of the right to name protection under the provisions of Art. 11 of the Civil Code is an exclusive right of a natural person to use a name, dispose of it, and prevent anybody else from using his or her name illegally, regardless of the purpose for which it would be used. This exclusive right can also be exercised by an individual by giving consent to the use of his or her name. However, someone using the name of a natural person without express consent would thus not only violate the fundamental right of an individual according

54 Constitutional Court, III. ÚS 193/2015 from May 12, 2015, decision, p. 11.
55 Ibid.
56 See Constitutional Court, III. ÚS 385/2012 from January 21, 2014, finding, p. 18.
57 Constitutional Court, III. ÚS 193/2015 from May 12, 2015, decision, p. 9.
58 See e.g., ECtHR, *Janowski* v Poland, application no. 25716/94, January 21, 1999.
59 Compare Constitutional Court, IV. ÚS 107/2010 from October 28, 2010, decision, p. 23.
60 Constitutional Court, PL. ÚS 12/97 from October 15, 1998, finding, p. 8.

to the provisions of Art. 19, para. 1 of the Constitution, but would also act in conflict with the provisions of Art. 11 of the Civil Code.[61] A natural person cannot lose a right to his or her name, and thus the right to dispose of it, by committing an offense and being punished for the offense under the Offenses Act.[62]

Right to a name and all other parts of this aspect of the privacy protection concern not only politicians but in a digital era anybody who enters digital world, either voluntarily or not. It includes consequences of the digital world substance in its broad and quick dissemination of facts and opinions. The right to name protection might be interfered with in a very profound and sometimes even unintended way. Therefore, the protection should include various forms and ways. In relation to the right to a human dignity, honor, and reputation protection it concerns especially vulnerable groups, one of which are children.

4. Right to privacy in digital era and children

Children are involved within constitutional private life protection from two sides. First, sometimes as victims. Generally speaking, Slovakia is a party to all the international treaties that deal specifically with the protection of children in the online world, to name the most important one, Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography. There has been general implementation procedure has been completed and child pornography and its (also online) dissemination have been made criminal.[63] Thus the most abusive forms of violation not only of the right to private life but also to privacy (separated under the Slovak Convention) have been legally processed and covered.

There are, however, other challenges to a right of a child to privacy. Although there has been no particular case law in the Slovak Republic dealing with the violation of the right to privacy of children as such, there have already been some cases on the international level,[64] and furthermore, not only purely academic discussion about how personal data of children are shared without their consent.[65] Of course, legally speaking, parents are legally responsible for their children until they become adults themselves. However, parents sometimes provide a name and even a date of birth of their children online without considering that it remains "out there" and that it can influence the future of their children in a negative way, not even speaking about pictures that might later cause humiliation feeling if found by

61 Ibid.
62 Ibid.
63 See e.g., paras. 368, 369 of the Criminal Code.
64 See e.g., ECtHR, *Reclos and Davourlis* v. Greece, no. 1234/05, 15 January 2009.
65 See e.g., Steinberg, 2017, pp. 839–884.

schoolmates.[66] At the age of four, most children are self-aware and therefore their perception of (digital) reality should be considered as well. Not only does it help to educate children about online access and communication, but it is also in their best interest.[67] Legally speaking, one might point out that it is a right exercised under the GDPR. However, GDPR application is legally binding only for members of the European Union, and in case of worldwide accessible social media, once the information crosses the EU's borders because of an automatically checked box giving consent, personal data may go to countries where they are not considered to be personal data but information provided for while exercising freedom of (parental) speech.[68]

This area is a new challenge and still under consideration. Although within the European regional system of human rights protection there have already been some cases dealing with consent in disclosure issues, most of them concern parental consent. As has already been indicated, there have already been some cases adopted on the international level. However, in *Reklos and Davourlis*, parents who claimed violation of the right to privacy of their child by taking a picture without their consent. Nevertheless, the consent of a child is to be considered as well because they have been recognized to a right to privacy themselves not only by general international treaties on human rights, such as the Convention, but also by a *lex specialis* international treaty, Convention on the Right of a Child.[69]

When speaking about children and their right to privacy, there is surely demand for their better understanding of interweaving of the real and digital world. The violation of basic human rights is forbidden in both; nevertheless, it might have broader consequences in the digital world because the digital world has broader and quicker reach. It is usually the area where children, although being considered as a vulnerable group, are proved to be perpetrators.

In case of perpetrators, one expects a proper fair trial and corresponding punishment. However, if children are included, the minimum age for criminal responsibility of children must be examined. Since there is no consensus among European countries on the minimum age of criminal responsibility of a child, each state has set up its minimum.[70] As for Slovakia, the Criminal Code of the Slovak Republic establishes the age as 14.[71] It means that whatever a child under 14 does, he or she cannot be held criminally responsible. The criminal responsibility of children considers the ability of children to bear consequences of their behavior and has been reduced in Slovakia to the age of 14

66 Another threat lies in misuse of personal data of children provided online by parents by higher risk of personal identity theft or financial fraud. See e.g., UK bank research. https://www.bbc.com/news/education-44153754.

67 See e.g., Art. 16, 18, para. 1 of the Convention on the Right of a Child.

68 Steinberg, 2017, p. 865; see also Stuart, 2014, p. 465.

69 Art. 16 of the Convention on the Right of a Child.

70 See the list of the minimum age for criminal responsibility: https://archive.crin.org/en/home/ages/europe.html.

71 Act no. 300/2005 Coll. Criminal Code, para. 22.

after recodification of the Criminal Code. If a child commits an act which otherwise would be defined as a crime and is not because of his or her age, s/he is not criminally responsible. If over 12, though, s/he might be given protective supervision.[72]

Criminal responsibility includes recognition and control elements. If they miss, the age limit is legally comparable to the state of insanity.[73] Nevertheless, children of today get matured sooner than before on both, the physical and mental levels, rapid technological development might have influenced this phenomenon as well. It is a usual situation that from the technological point of view, children are best to assist their parents.[74] On the other hand, threats of the functioning of the digital world are better known by parents because of their life experience.

The Slovak legal order has finally addressed the issue of cyberbullying. It has been several years since the Criminal Code allowed criminal prosecution of *de facto* cyberbullying by the *de iure* prosecution of several other already defined crimes. *De facto* cyberbullying has been prosecuted by cyberstalking, blackmail, coercion, sexual abuse, defamation, violation of others" rights, child pornography (production, distribution, possession), endangering morality, endangering the moral upbringing of young people, even by prosecution of the crime of the support and promotion of groups working to suppress fundamental rights and freedoms, crime of the production, dissemination and preservation of extremist material, crime of the denial and approval of the Holocaust and crimes of political regimes, crime of defamation of nations, races and beliefs, crime of incitement to national, racial and ethnic hatred, and crime of incitement, defamation, and threats to persons based on their race, nation, nationality, color, ethnic group, or origin.[75]

Nevertheless, the substance of bullying differs from the aforementioned crimes. The aim of bullying is to humiliate or even exclude an individual from a particular social environment. Nevertheless, although the aim of cyberbullying is the same as in the case of bullying, cyberbullying is even more invasive than "traditional" bullying.

First, there is no time or space limitation. So-called traditional bullying is usually limited to one space, e.g., school or work; nevertheless, in the case of cyberbullying, attacks with an aim to humiliate can come anytime and anywhere, the only barrier is a no mobile or no Internet access. Furthermore, its spread is much quicker and broader. It does not affect only those present, not only it can quickly reach a large amount of people, but its distribution is uncontrollable. Another difference is related to anonymity. Perpetrators can feel safer and even less aware of what their behavior causes because they do not see the victim's reaction, they miss the possibility of human empathy that is missing especially in case of social or psychological pathology. Moreover, for the victim, the anonymity of the perpetrator contributes to even greater

72 Ivor, Polák and Záhora, 2021, p. 144.
73 Ibid.
74 Children are considered to be digital natives, see e.g., Kurucová, 2018, pp. 127–135.
75 For the definitions of these crimes, see the Criminal Code. As for the list, https://www.kybersikanovanie.sk/index.php/legislativa.

suspicion, uncertainty, and fear since there might be cases when s/he does not know who to defend against, s/he does not know where the next attack will come from since the perpetrator can be anyone. Finally, cyberbullying overcomes differences more easily, because of anonymity and the use of technical means, it is easier for perpetrators to attack someone they would not have dared to in the real world because of their authority or position. It means that even adults might become a victim of cyberbullying by children. Finally, unlike traditional bullying, the perpetrator and the victim are not in direct contact, so after cyberbullying there are no visible traces of physical harm although physical harm might be even more serious.[76]

Considering all these differences, one admits the special danger of cyberbullying that must be dealt with by special means of criminal law. It is one of the effective ways how a state might fulfill its positive obligation under Art. 8 of the Convention. Because of a criminal principle of *nullum crimen sine lege*, a new crime had to get defined to allow police and other law enforcement authorities to prosecute cyberbullying. It was done so by an amendment of the Criminal Code in 2021 when a new crime was incorporated into the Criminal Code, namely the crime of dangerous electronic harassment. As it has already been, the crime of cyberbullying is specific because of the intent to humiliate a victim. It is one of the features that must be met if a person is to be prosecuted for this crime.

To analyze this important step of right to privacy protection under Slovak framework requires a precise definition:

> Who intentionally degrades the quality of life of another by means of an electronic communications service, computer system or computer network by:
> (a) degrading, intimidating, acting on his/her behalf or otherwise harassing him/her[77] on a long-term basis; or
> b) unjustifiably publishing or making available to a third party a visual, audio, or audio-visual recording of his/her personal presentation obtained with his/her consent, capable of significantly jeopardizing his/her seriousness or causing him/her other serious harm to his/her rights,
> will be punished by imprisonment for up to three years. [78]

To sum up definitional elements of the new crime, there must be: the intent, longevity, degradation, intimidation, harassment, or serious harm to the rights of a victim, and finally, a significant deterioration in the victim's quality of life.

Although a part of the definition of the new crime, there is no additional definition of the degradation or intimidation. Consequently, keeping in mind the Court's

76 Compare https://www.zodpovedne.sk/index.php/sk/ohrozenia/kybersikanovanie.

77 Slovak language distinguishes three linguistic genres: male, female, neutral. Within legal text, male version of "who" and "other" is used, "her" has been added preventively here by the author to make sure that no one is excluded within understanding of a reader.

78 Para. 360b of the Criminal Code.

explanation,[79] definitions used in the Convention's interpretation by the ECtHR should be used. Therefore, treatment that is intended to humiliate or debase an individual, showing a lack of respect for or diminishing their human dignity, or arouses feelings of fear, anguish, or inferiority capable of breaking an individual's moral and physical resistance, is considered degrading.[80] Furthermore, behavior can be considered intimidating when the aggressor arouses fear or apprehension in the victim that certain harm will occur on his/her side, regardless of whether that harm is to occur immediately or to be inflicted later.[81]

When preparing the amendment, it was expected that the explicit regulation of the specific crime of dangerous electronic harassment will undoubtedly facilitate the derivation of responsibility for aggression through communication services and social networks. Nevertheless, as usually, practical application means unexpected challenges as proved in the following example.

Slovakia was shocked by an incident that took place in Miloslavov, a town in the western part of the Slovak Republic. Several children, aged 14, 15, and 16, assaulted an 11-year-old girl by beating her, getting her drunk, and after undressing her, they recorded her and published the video on social media.[82] Immediate response from all the authorities responsible for children took place, including psychologists *in situ*. Nevertheless, questions have remained concerning punishment.

There were allegedly 10 perpetrators present at the place of the attack, one of whom was younger than 14 and therefore could not be held responsible. All the other attackers were expected to be prosecuted for several crimes, those who had published videos online and participated in their dissemination, especially for cyberbullying. However, the situation has been proved to be more complicated since the newly adopted amendment of the Criminal Code on cyberbullying is not applicable.

There is no doubt that the trauma suffered by the 11-year-old girl is doubled. First, the brutality of the attack has fundamentally violated her right to inviolability of a person under Art. 16 of the Constitution. Second, videos of the assault quickly began to spread on the Internet. Although the investigation is still ongoing,[83] so far only the attack itself can be prosecuted, not the dissemination of videos that were recorded and later published. The problem is the element of consent in the new crime of dangerous electronic harassment. It only applies to videos that were acquired with the consent of the person but have been published without their consent. The video under investigation has been recorded without the consent of the assaulted girl.

As for this current case, "only" traditionally used crimes are available to be prosecuted, such as aforementioned crimes of defamation, violation of others' rights, child pornography (production, distribution, possession), endangering morality,

79 See e.g., Constitutional Court, PL. ÚS 5/93 from 18 May 1994, decision, pp. 10 et seq.
80 See e.g., ECtHR, *M.S.S.* v. Greece and Belgium, 2011, no. 30696/09, para. 220.
81 Compare Ibid.
82 See e.g., https://www.zenyvmeste.sk/miloslavov-dievca-napadnutie-kamarati-sikana.
83 This part of the chapter is being written in April 2022.

endangering the moral upbringing of young people. The police have already informed that the leader of the group is accused of the crime of injury to health and the crime of rioting.[84] This 16-year-old girl faces half the sentence compared to the situation if she committed the same crime as an adult.

Nevertheless, as for the possible applicability of the new crime to similar situation *pro futuro*, another amendment of the Criminal Code should be adopted that would concern consent. It is a clear demand for proper and effective protection of the right to privacy. Bullying is becoming increasingly common in the online space and has been proven to be a huge problem despite all kinds of national plans and other ways of criminal prosecution as mentioned above. The new wording of the crime should therefore also deal with finger-pointing, intimidation, humiliation, or sharing of private photos and videos via the Internet, especially in the cases in which the victim did not give consent.

Bullying most often occurs in the real world. From here, conflicts are also transferred to the digital world. It follows that the prevention of cyberbullying is to develop relationships, to work on solving conflicts and to increase the ability to empathize with the experiences of others.[85] Having said that the cyberbullying has been the case when children are often seen as perpetrators, it is very important to point out that cyberbullying is present also among adults. Specific regulations must have been adopted to prevent right to privacy violation e.g., in case of employees.

5. Right to privacy and unauthorized monitoring

Even if not at the level of bullying, the right to privacy might be violated also by other means, such as monitoring.

Right to privacy in general is protected by Art. 16 of the Constitution and broadened by *lex specialis* within Art. 19 of the Constitution and Art. 22 of the Constitution. The former concerns protection against unauthorized collection, publication, or other misuse of personal data,[86] the latter focuses on protection of personal data as such.[87] Although the subject of the protection is the same, personal data, they

84 Information provided by police in their Facebook status. https://www.facebook.com/KRPZBA/photos/a.604815706607630/1373949529694240/?type=3.

85 See further recommendations: https://www.zodpovedne.sk/index.php/sk/ohrozenia/kybersikanovanie.

86 See Art. 19, para. 3 of the Constitution.

87 See Art. 22 of the Convention: "(1) The privacy of letters and secrecy of mailed messages and other written documents and the protection of personal data is guaranteed. (2) No one may violate the privacy of letters and the secrecy of other written documents and records, whether they are kept in privacy, or sent by mail or in any other way, except for cases which shall be laid down by law. Equally guaranteed is the secrecy of messages conveyed by telephone, telegraph, or other similar means.".

pursue a different goal, as if Art. 22 of the Convention was *lex specialis* in relation to Art. 19 of the Convention since it guarantees protection against secret surveillance of communication.

Nevertheless,

> by limiting the protection of personal data to protection against unauthorized processing of personal data, the Constitution implicitly allows for the legitimate processing of personal data. The Constitution does not preclude any collection of personal data.
> Protection is granted only against unauthorized collection, disclosure, or other misuse of data. Legally collected data must be stored by a public authority in such a way that they are protected from unauthorized access by other public authorities, including natural and legal persons. If a public authority collects data on a person who is not entitled to identify, store, or otherwise obtain in its disposal sphere, it shall commit conduct inconsistent with Art. 8, para. 2 of the Convention. The state of technology making it difficult to access data or other measures taken to protect the data stored in the information system cannot be confused with the protection against unauthorized collection of personal data.[88]

The relationship between Art. 19 and Art. 22 of the Convention is very important since it has influenced the methodology of examination whether there has been unlawful interference into personal data protection. First, application of Art. 22 of the Convention is analyzed by reviewing whether there has been secret surveillance of personal data. Even if not, use of personal data reviewed under Art. 19 of the Convention follows. It has been so e.g., in case of constitutionality check of some articles of the Act on Electronic Communication.[89] Technological development has enabled various ways of data collection, nevertheless, not everything that is technically possible is legally in accordance with the Constitution although the law may even require it. The amendment of the Act on Electronic Communication has imposed an obligation on electronic communications providers to retain traffic, location, and communicating party data from the date of the communication for six months for Internet connections, Internet e-mails, and Internet telephony, and for twelve months for other types of communication.[90] Although it was not a question of monitoring the content of the communication as such, it is also possible to obtain information of a personal nature within the framework of profiling from the aforementioned information, as has been pointed out by the Court since

> from the above data on users, recipients, exact date, time, and duration of communication, type of communication, data related to terminal identification, or data

88 Constitutional Court, III. ÚS 400/2016 from November 29, 2016, finding, p. 7.
89 See Constitutional Court, PL. ÚS 10/2014 from 29 April 2015, finding.
90 Act no. 351/2011 Coll. on Electronic Communications.

> needed to identify the location of a mobile terminal; relatively detailed information on social or political affiliation can be compiled in their mutual combination, as are personal hobbies, health, sexuality, and the inclinations or weaknesses of individuals. From the data that electronic communications providers are obliged to retain, it is also possible to draw sufficient content conclusions that fall within the private sphere of the individual.[91]

Moreover, the

> considerable intensity of the invasion into the right to privacy was also due to the fact that the stored data and their subsequent use without informing the subscriber or registered user might make the persons concerned feel that their private life is subject to constant monitoring.[92]

As soon as the Court finds interference into the private sphere of the individual, it admitted the legitimate aim of crime prevention and protection of public security; however, when applying the test of proportionality, it found it in violation of the constitutional protection of the right to privacy. Not only did the examined regulation apply to all participants and registered users, including those not indirectly involved in a situation that could lead to criminal prosecution, and even those whose communications under the relevant legislation are subject to professional secrecy or to a duty of confidentiality established or recognized by law,[93] "the objective pursued by the contested legislation in supporting the fight against serious crime and, ultimately, public security could also be achieved by other means which constitute a less intensive invasion of the right to privacy."[94] The Court noted other tools that it considered more appropriate than the widespread and preventive retention of the relevant data, such as the so-called data freezing, which after meeting the specified conditions, is allowed to monitor and store the necessary and selected data only with a specific, predetermined participant in the communication.[95] Moreover, the Court also objected to insufficient safeguards and means of protection for the individuals concerned to effectively protect personal data against the risks of leaks, misuse, or any illegal access or illegal use of this data.[96]

Although there is a legal definition of personal data as

> data relating to an identified natural person or an identifiable natural person which can be identified directly or indirectly, in particular by a generally applicable identifier, another identifier such as name, surname, identification number, location data,

91 See Constitutional Court, PL. ÚS 10/2014 from 29 April 2015, finding, para. 106.
92 Ibid. para. 107.
93 Ibid. para. 120.
94 Ibid. para. 122.
95 Ibid.
96 Ibid.

> or an online identifier, or based on one or more of the characteristics or traits that make up its physical identity, physiological identity, genetic identity, mental identity, mental identity, economic identity, cultural identity or social identity,[97]

the Constitution provides protection also for legal persons. Furthermore, not only data collection itself, but also the way how the data are collected is important. Monitoring of a public space and not intentional or intentional data collection in such a case even if a person is not aware of it is not violation of the right to privacy according to Art. 19 neither Art. 22 of the Constitution if it done on a legal basis.[98] However, there might be a problem with use of the data if collected systematically and intentionally. Furthermore, special protection is provided to the communication between an advocate and his or her client.[99]

Although several years ago, *Kvasnica* (decided by the ECtHR) is a perfect example of not only secrecy surveillance problem but also of leaking information including personal data from official bodies.[100] This case was selected not only because of the ECtHR decision but also because of a rather often situation also in the current Slovak media attitude to online publication of information not supposed to be shared

97 Act no. 18/2018 Coll. on Personal Data Protection, para. 2.

98 Orosz and Svák, 2021, p. 246.

99 Communication between an advocate and a client is included also in documents that are especially protected. Nevertheless, they might be sometimes seized. Since the amount might be huge in electronic version, specific rule is to be observed. As the Constitutional Court in its decision no. II. ÚS 96/2010 from February 3, 2011, p. 32, observes, "Digital world and related technological development have enabled various forms of data collection, including for the purposes of criminal investigation, such as complete data extraction from notebooks, mobiles, or other data carrier, including those that are not relevant for a particular criminal case. The question is therefore appropriate what the balance between interference into the right to privacy and necessity is to conduct effective criminal investigation when huge amount of data need much time to get examined to select the relevant part. The Court has been consistent by pointing out the Criminal Procedure Code whose systematic interpretation allows isolation of data relevant to criminal proceedings and subsequent disposal of a copy containing the complete set of data recorded on the storage medium, or its return to the relevant individual." The Court has thus applied existing legal rules appropriately what has been confirmed in its decision no. IV. ÚS 210/2020 from May 26, 2020, paragraph 66, in which it has elaborated the time element and proportionality principle and decided that "data extraction without prior selection is constitutionally acceptable form of execution of the order for storage and issuance of computer data. Lengthy analysis of data on various material carriers in the place where the house search is performed, respectively inspection of other premises, for the purpose of extraction of only selected data, or removal of material carriers themselves and subsequent thorough data selection and extraction and copying of only selected data represent a much more invasive intervention compared to surface data extraction without their previous selection. After such surface extraction, the procedure according to §90 para. 3 of the Criminal Procedure Code, which allows the interpretation that this procedure may also be applied to a part of the computer data obtained, i.e., if a certain part of the data is reliably established by selection and analysis, that they are not necessary for the purposes of criminal proceedings, e.g. because they have nothing to do with the matter, the order to cancel the retention of this data may be applied to the specified group of data, depending on the specific circumstances, it is not necessary to wait for the selection of the entire volume of data.".

100 ECtHR, *Kvasnica* v. Slovak Republic, application no. 72094/01, June 9, 2009.

because of being a part of criminal prosecution.[101] Moreover, as with the *Kvasnica* case, even in the current Slovak public space, there has been a conflict within security forces that is partially realized by having information leaked.[102]

As for the facts of the *Kvasnica* case, the complainant was a lawyer, an active advocate at the time. Between August 1999 and March 2001, he acted as a lawyer for several industrial companies belonging to the group associated with strategic steel mills in eastern Slovakia, and from April 18, 2001, he was on the board of directors of the company that owned the factory. In 1999, the Minister of the Interior set up a specialized investigation team to clarify the extensive organized criminal offenses of a financial nature which were committed in connection with a company belonging to the above group.

The investigators asked the court to consent to the interception of the applicant's telephone, and the judge of the Regional Court in Bratislava granted the request. Subsequently, calls from and to the complainant's mobile phone were intercepted.

In November 2000, the applicant learned that calls from his telephone had been recorded, that the interception was carried out by the financial police, and that the content of his telephone communication was known outside police environment. On January 5, 2001, the applicant received an anonymous letter confirming the above information and stating that the interception took place from October to December 2000, upon request of opponents of his clients. On May 31, 2001, and June 1, 2001, a newspaper published an interview with the Minister for the Interior and the head of the president's police force. From the content of these interviews, the complainant understood that they confirmed that his interception had taken place. Moreover, transcripts of the applicant's interviews leaked and were made available to various interest groups, politicians, and journalists as well as representatives of several legal entities.

In the summer of 2002, the applicant was informed that transcripts of his interviews with third parties recorded by financial police are freely available on the Internet. These transcripts included his interviews with colleagues, clients, representatives of the other party to the proceedings and friends. The transcripts have been amended to include statements which the complainant and the other persons concerned did not make.

Not only the applicant but also the director of the special division of the financial and criminal police lodged a complaint based on violation of relevant domestic legal norms. Nevertheless, the judge who had authorized the interception made a written statement to the president of the regional court stating that the request for the authorization had met all formal and substantive requirements. He admitted though that

101 There is a conflict between a right of public to information (usual media claim) with a right to a fair trial (usual lawyers and their clients claim). Nevertheless, such a conflict (especially in relation to the principle of proportionality) should be decided by an independent court, not by public mood. See e.g., https://zurnal.pravda.sk/neznama-historia/clanok/607289-pozor-na-uniky-informacii/.

102 See e.g., https://spravy.rtvs.sk/2021/06/inspekcia-ministerstva-vnutra-zasahovala-v-naka-k-zasahusa-vyjadril-aj-minister/.

requests for authorization were made in writing but were submitted in person and that oral presentation was usually more comprehensive than the written request. Moreover, he pointed out that judges had to rely on the information in the request for authorization, which presupposed a certain level of trust.

Although there were other complaints submitted by the applicant, no information about the investigation's result was served on him. He even submitted criminal complaints, but they were all rejected, apart from one that was started by a police officer who was later asked to leave the police force for not respecting a general order within the police corps to reject all of the applicant's complaints. Finally, the government submitted a position paper of the general prosecutor which stated that all decisions had been taken in accordance with the law.

Since the complainant did not exhaust all effective domestic remedies (specifically a complaint possible under Civil Code, Art. 13), the ECtHR declared inadmissible his complaint about interference resulting from the copying, misuse, distribution, and publication of the transcripts of his telephone conversations. Nevertheless, as for the interception itself, it found that Art. 8 of the Convention was violated for several reasons. First, according to the ECtHR, it has not been shown that the guarantees relating to the duration of the interference were met, whether there had been judicial control of the interception on a continuous basis, whether the reasons for the use of the devices remained valid, and whether in practice measures were taken to prevent the interception of telephone calls between the applicant as a lawyer and criminal defendants as his clients. Moreover, the ECtHR found that it had not been shown that the interference restricted the inviolability of applicant's home, the privacy of his correspondence, and the privacy of information communicated only to an extent that was indispensable and that the information thus obtained was used exclusively for attaining the aim set out by law. Furthermore, statements by several police officers and the judge involved were indicative of several shortcomings regarding compliance with the relevant law in the applicant's case. In particular, the director of the special division of the financial and criminal police had concluded that the interference at issue had not been based on any specific suspicion against the applicant and no specific purpose had been indicated in the relevant request. In addition, as it has already been indicated, the judge who had authorized the interception remarked that similar requests were made in writing but were submitted by the police investigators in person, which made the request more comprehensive. Finally, there was the information involved that the request for authorization of the interception of the applicant's telephone had been drafted without a prior consultation of the case file and the documents before the Court contained no information indicating that those statements were unsubstantiated.[103]

Apart from this specific problem with unauthorized interception within criminal matters, there has been special legal area that concern much more people in their

103 Ibid. paras. 86, 87.

ordinary working lives, namely legal regulation of a relationship between an employee and an employer.

It is true that the Labor Code does not contain a comprehensive legal regulation concerning the protection of the personality of a natural person, including his or her right to privacy as the Civil Code does. However, some selected provisions of the Labor Code are, in essence, aimed at the protection of individual personal rights such as the right to privacy or the right to the protection of the health and life of a natural person. Nevertheless, when assessing the protection of the employee's personality in an employment relationship, attention should be paid to the possibility of applying the above provisions of the Civil Code first and subsequently to individual provisions of the Labor Code according to which "unless this Act provides otherwise in the first part, the general provisions of the Civil Code shall apply."[104]

In addition to the protection under the Convention and the Civil Code, there are several provisions of the Labor Code that are aimed at the protection of employees and their privacy. As far as the control of employees by the employer is concerned, i.e., by monitoring in a form of the collection of information, it is possible to speak of an interference with the personal life of the employee. Pursuant to Art. 11, which forms one of the basic principles laid down by the Labor Code, the employer may only collect personal data about the employee related to the employee's qualifications and professional experience and data that may be relevant to the work the employee is to perform, perform or has performed.

A distinction must be made between the collection of information and data by the employer before and after the employment of the employee. As for the former, Art. 41 of the Labor Code regulates the relations between the employer and the employee. First, in a positive way when it indicates what the employer may request from the natural person applying for the job, i.e., only information that is related to the work s/he is to perform.[105] The employer may require a natural person who has already been employed to submit a work report and a certificate of employment. Second, in a negative way when it defines data that the employer cannot request from a natural person, such as information on pregnancy,[106] family circumstances, or political affiliation, trade union membership, or religious affiliation.[107]

If the employment relationship has been established, the employer has a different position in obtaining information about the employee.

In accordance with the general principles of legality, legitimacy and proportionality, employee monitoring will be lawful only if such control is required by law and will be carried out only to the extent and to the extent provided by law. Monitoring of employees is legitimate only if the employer fulfills its obligation to notify

104 Act no. 311/2001 Coll. Labor Code, Art. 4 para. 1.

105 See Art. 41, para. 5 of the Labor Code.

106 However, pursuant to Art. 40, para. 6 of the Labor Code, only an employee who has informed the employer in writing about the pregnancy is considered a pregnant woman. Fulfillment of the information obligation is conditional on its special legal protection.

107 See Art. 41, para. 6 of the Labor Code.

the employee and notifies him or her in advance of the existence of the inspection, the scope of the inspection and the form and manner of the inspection. The principle of proportionality will be respected if the inspection is carried out only to the extent necessary, for example to respect occupational health and does not infringe the human dignity of the employee.

Keeping in mind technological development and technological monitoring possibilities, it must be pointed out that as it has already been referred to, Act on personal data protection defines what personal data are, however it provides only a demonstrative calculation. Therefore, the IP address of the Internet connection being used might be considered personal data as well.

To indicate expressly stated legal protection, according to Art. 13 para. 4 of the Labor Code, the employer may not infringe the employee's privacy at the workplace and in the employer's common premises without serious reasons due to the special nature of the employer's activities by monitoring him, recording telephone calls made by the employer's technical work equipment and checking e-mail sent from the work e-mail address and delivered to this address without notifying him in advance. If the employer implements a control mechanism, he is obliged to discuss with the employees' representatives the scope of the inspection, the method of its implementation, as well as its duration and inform the employees about the scope of the inspection, the manner of its implementation and its duration. To be more specific, serious reasons, as defined in that provision, must in each case be assessed individually, depending on the nature of the work, the place of work and the like.

The overall protection by the Labor Code therefore allows the employer to control the work activities of its employees, but s/he must choose appropriate means and forms that do not conflict with the legislation protecting the employee's privacy. For example, the camera system can be used by the employer, provided that the protection of the employee's privacy is not infringed and if the purpose pursued by the employer cannot be achieved otherwise. The aim of the employer might be also control compliance with the working rules, however, the employee must be informed by the employer about the camera monitoring, namely its scope, time duration and the manner of its implementation.

As regards the monitoring of electronic mail, in accordance with the mentioned Art. 13 para. 4 of the Labor Code, the employer may not, without serious reasons based on the special nature of the employer's activities, infringe the employee's privacy at the workplace and in the employer's common premises, by checking e-mail sent from and delivered to the work e-mail address unless warned in advance.

Those serious reasons in such a case also must be assessed individually in the case of e-mail tracking about the subject and activity of the employer, for example the protection of the employer's intangible assets, such as trade secrets. Nevertheless, before the employer carries out the employee's e-mail check, he or she must present those serious reasons and inform the employee about the scope, method, and duration of the e-mail check.

Nevertheless, if the employee considers that the monitoring is illegal and his or her private life or personality rights have been violated, s/he has the right to submit a complaint to the employer who is obliged to respond to the employee's complaint without undue delay, to make a correction, to refrain from such action and to eliminate its consequences.[108]

The employer may regulate in its internal regulations the use of electronic mail by employees. When using Internet access and e-mail services, the employee is obliged to comply with applicable laws and internal regulations of the employer, which may include various restrictions, such as the use of e-mail not violating the job's rules or activities that conflict with and unrelated to the employer's business. On the other hand, an employer may allow an employee to use e-mail and Internet access for any private purposes.

As for monitoring of telephone calls, it might be exercised to prevent employees to use a work telephone for private purposes. Nevertheless, privacy must be observed when monitoring telephone calls, it means that the content of telephone calls must remain confidential, the employer can only check called numbers.

The employee's liability arises when s/he commits an illegal act or a breach of duty, a breach of work discipline consisting e.g., in the use of official equipment for private purposes.

Personal inspection of the employee by the employer can also be understood as monitoring of the employee: its purpose in practice lies in the prevention of removal of inappropriate things to and from the workplace.[109] More detailed conditions must be determined by the employer in the working rules, first, personal inspection must be carried out at the workplace and during working hours, otherwise the employee's right to privacy would be violated. Moreover, protection of personal liberty must be observed during the inspection and human dignity must not be degraded.

6. Right to privacy and unauthorized registration of personal data

Apart of monitoring, two specific cases have been selected to be analyzed in relation to the issue of the right to privacy within data collection and processing. The first was decided by the ECtHR and is related to the violation of Art. 8 of the Convention. The second was decided by the Court of Justice and was based on an analysis of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and on the right to privacy protection in relation to processing of personal data laid down in Directive 95/46/EC (1) of the European Parliament and of the

108 Compare Art. 13, para. 6 of the Labor Code.
109 Ibid. Art. 177, para. 2.

Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

As for the first one, it deals with specific situation referring to existence of so-called StB files and registration within them. During the Communist regime, the State Security Service (Štátna bezpečnosť, or StB) held its files with lists of collaborators. Those collaborators were divided into several groups based on the level of their cooperation, such as agents or candidates for cooperation or informant.[110] After the fall of the Communist regime, those StB files were made available (although some were destroyed) and several people realized they were within the lists without giving their consent to cooperation.

There were several cases decided by both supreme courts of the Slovak republic, some of them dealing with the issue of passively legitimacy of an entity in proceedings for the protection of the personality of a natural person registered in the StB files, i.e., who is responsible for interference into personality rights.[111] At the beginning, it was Slovak Intelligence Service that was under the control of Ministry of Inferior that was in charge of administration of the files, later on, this administration duty has been transferred to the Institute of the Memory of the Nation. The Institute is not a state body; nevertheless, in accordance with legal obligations, it was imposed to make all the handed over documents available, to publish all the relevant data and provide the necessary information designated by the public authority.[112] According to the Supreme Court, it has been held at the same time as the entity responsible for the risk associated with these tasks, if the data in these materials, respectively registration in them, is unjustified, even though it has not been expressly so identified in the legal act.[113]

Identifying who is responsible for the unjustified registration and therefore unjustified processing of personal data has taken several years and judicial bodies to get the final decision. The Constitutional Court finally decided upon the status of the Institute and its responsibility in relation to the claimed interference in personality rights of allegedly unjustifiably registered individuals.[114]

According to the Court, the mere fact that a body (a public body) has become *ex lege* the holder of physical media on which the outputs of (official) activities of public authorities are captured does not in itself constitute a transfer of responsibility for the unjustified interference with the right to protection of personality which might have taken place.

The Court has pointed out that the general courts appear to have relied on the considerations set out in one by which passive legitimacy was referred to the Slovak

110 See e.g., website of the Institute of the Memory of the Nation that provides information about several categories of collaborators. https://www.upn.gov.sk/sk/vysvetlivky-k-registracnym-protokolom/.

111 See e.g., Supreme Court of the Slovak Republic, 6 Cdo 83/2010, decision from 31 May 2011.

112 Act no. 553/2002 Coll. on the Institute of the Memory of the Nation.

113 Supreme Court of the Slovak republic, 6 Cdo 83/2010, decision from May 31, 2011, p. 5. See also Supreme Court of the Slovak Republic, 5 Cdo/83/2008 from November 27, 2009.

114 Constitutional Court, II. ÚS 285/2017 from October 12, 2017, finding.

Intelligence Service. However, at that time, the Slovak Intelligence Service was a state body, i.e., a body acting on behalf of the state. Moreover, in that case, it was not a matter of determining the originator of the intervention and the responsible person, as it was not disputed that the originator of the intervention was the state; it was therefore only a matter of designating a state body, which has passive legitimacy.[115] However, the Institute is not a state body and therefore the relationship between the persons registered in the StB files and the public authority clearly cannot be described as private, and therefore no personality protection based on Civil Code applies to them.[116]

In addition, the Court has analyzed a possible reasoning that it was not the registration but the publication of the files that interfered with the individual's rights within the meaning of Art. 13 of the Civil Code, i.e., by the act of publishing an already existing information or document. It means that although individual allegedly did not cooperate, the information claiming the opposite has been published without having been proved. The Court has not ruled out in general terms that an intervention within the meaning of Art. 13 of the Civil Code may also consist in the publication of information obtained by a state authority in the performance of its statutory tasks. In this context, however, Art. 13, para. 1 of the Civil Code explicitly provides protection (only) against unauthorized interference.[117]

The Act on the Institute of the Memory of the Nation established the public constitution (as well as other public institutions), and empowered it to perform tasks of a public nature, in this case related to dealing with the past. Art. 19 para. 1 of this Act stipulates the obligation of the Institute to publish in print and on electronic media a transcript of records from preserved or reconstructed files. The Court has repeatedly emphasized that the Institute has no discretion in publishing registration protocols, i.e., the right to decide whether to publish a part of them. The Institute does not even rewrite the data in these protocols (where a transcript might be erroneous). The Institute's liability for examining the correctness of the materials entrusted to it is expressly excluded by Art. 26, para. 3 of the specified Act on the Memory of the Nation, according to which "the Institute is not obliged to verify whether the data contained in the document and the data obtained in the information system of documents from the preserved records referred to in paragraph 2 are accurate or true." Fulfillment of this legal obligation is therefore precluded, and by fulfilling it, the Institute acted unlawfully, i.e., that such disclosure (if made exactly in accordance with Art. 19 and other provisions of the Act on the Memory of the Nation) may constitute unjustified interference within the meaning of Art. 13, para. 1 of the Civil Code.[118]

115 Ibid. paras. 28, 29.
116 Ibid.
117 Ibid. paras. 32 et seq.
118 Ibid. paras. 32, 33.

Nevertheless, there have been cases when individuals asked to be deleted from the StB registration files—some of them successful.[119] However, in the selected case, Mr. Turek has had to face more challenging rules.[120]

Mr. Turek worked in the state administration of the school system. He occupied a leading post that fell within the purview of the Lustration Act,[121] which defined some supplementary requirements for holding certain posts in public administration. In January 1992, the applicant's employer asked for a clearance concerning the applicant and received a negative one. It meant that the applicant was disqualified from holding certain posts in public administration, so he resigned from his post, later he left his employer completely, having felt compelled to do so. The information about who was registered in the StB files has been made public in newspapers and online. In May 1992, the applicant lodged an action for protection of his good name and reputation; he alleged that his registration as a collaborator was wrongful and unjustified.

The applicant admitted having met StB agents several times before and after his journeys abroad, when they had instructed him on how to behave abroad and asked for information about his stay. Nevertheless, according to the applicant, their discussions were of a general nature and included the situation at the applicant's workplace. The applicant admitted having obtained and provided a list of students who had been preparing for studies abroad; however, he considered information public in any case. He had never had the impression that he was considered a collaborator and had never been asked to keep his contacts with StB officers' secrets.[122]

The lower national courts established that the applicant's meetings with StB agents amounted to formal collaboration, and that the applicant had failed to prove that that his registration as a collaborator had been contrary to the rules applicable at the material time. Moreover, the Supreme Court held that the fact that the applicant was registered in the StB files did not by any means constitute evidence that he had been a conscious collaborator of the StB. In addition, in line with established judicial practice, the Supreme Court noted that the procedure concerning the issuance of a security clearance under the Lustration Act could not amount to a violation of an individual's good name and reputation, since only unjustified registration in the StB files would amount to such a violation. The Supreme Court considered that it was crucial for the applicant to prove that his registration had been contrary to the rules applicable at the material time and concurred with the lower courts' conclusions that the applicant had failed to do so.[123]

119 These were cases when an individual had to prove that the official registration information was fabricated already at the time it was done, e.g., by including fake information by the police agents themselves. See e.g., a story of František Krajňák, 2014. https://zivot.pluska.sk/pribehy/knaz-frantisek-krajnak-ocistil-svoje-meno-nebol-agentom-stb. However, as it is pointed out in the article, as a result, even if there was a judgment of the Court, the name is not deleted from the list, the Institute only upload the judgment on its website. On the contrary, if a claimant is successful in the Czech Republic, his or her name is deleted from the registration file.

120 ECtHR, *Turek* v. Slovakia, no. 57986/00, February 14, 2006.

121 Act no. 451/1991 Coll. Lustration Act.

122 ECtHR, *Turek v. Slovakia,* no. 57986/00, February 14, 2006, para. 48.

123 Ibid. para. 57.

As for the ECtHR proceedings, the most important argument in relation to the alleged violation of Art. 8 of the Convention was the applicant's claim that during the lustration proceedings, he had been denied access to guidelines that defined the category of "agent" and established rules of cooperation with agents, since the document was classified "top secret."

The ECtHR did not follow the Supreme Court's decision about non-violation of an individual's good name and reputation, it observed that the applicant's registration as a StB collaborator affected his name and reputation and therefore interfered with the requirements of Art. 8 of the Convention. The ECtHR then decided whether the interference was justified, examining whether the procedural protection at the domestic level of the right of Mr. Turek to respect his private life was "practical and effective." The Court acknowledged that there may be legitimate grounds to limit access to certain documents and other materials. However, the Court concluded that denial of access to the requested information in the circumstances of the instant case was unnecessary for three reasons.

First, the Court stated that the nature of lustration proceedings indicates that they are oriented towards the establishment of facts dating back to the Communist era, and they are not directly linked to the current functions and operations of the security services. Thus, "it cannot be assumed that there remains a continuing and actual public interest in imposing limitations on access to materials classified as confidential under former regimes."[124] Secondly, due to the nature of the lustration proceedings, if the applicant to whom classified material relates is "denied access to all or most of the materials in question, his or her possibilities to contradict the security agency's version of the facts would be severely curtailed."[125] Finally, since the respondent in the lustration proceedings is the security agency, which has the power to decide what materials should remain classified and for how long, "This power is not consistent with the fairness of the proceedings, including the principle of equality of arms."[126] The Court therefore concluded that the domestic courts placed an unrealistic burden on the applicant, since he was required to prove that his designation as a collaborator was unjustified without having access to the applicable rules, while the state did have full access.[127]

Another very specific case dealing with the right to privacy protection because of alleged unlawful or unjustified registration of an individual concerns a case decided by the Court of Justice. It had been decided before the GDPR adoption, therefore based on the analysis of the Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and also on the analysis of the Charter of Fundamental Rights of the European Union, Arts. 7 (protection of the right to respect for private and family life, home and communications), 8 (protection of the right to the

124 Ibid. para. 115.
125 Ibid.
126 Ibid.
127 See also the summary. https://globalfreedomofexpression.columbia.edu/cases/turek-v-slovakia/.

protection of personal data), and 47 (protection of the right to the effective remedy). In the decision, the Court of Justice had to deal with a request for a preliminary ruling from the Supreme Court of the Slovak Republic. The case concerned a dispute between Mr. Peter Puškár and the Finance Directorate of the Slovak Republic and the Criminal Financial Administration Office upon a list of persons considered by the Finance Directorate to be the so-called "white horses," i.e., people to whom a legal entity is assigned, in which the white horse is "active" with the birth number of the white horse, the tax identification number of the tax entity in which the white horse is active, and the "functional" period of the white horse.[128] White horses are persons who only lend their first and last name and their identity to assume rights and obligations that they have no real interest in exercising. This concept is used unofficially to identify individuals that are usually misused by third persons to exercise unfair exercises. The mentioned applicant asked in the case for an order requiring those authorities to remove his name from the list created in the context of tax administration. The Court of Justice was asked four preliminary questions, one of which is relevant for the research area.[129]

The basis of the question lies in the interpretation of the directive and Art. 7 and Art. 8 of the Charter in relation to the legal possibility of a Member State to create, without the consent of the person concerned, a register of personal data for the purposes of tax administration, so that the fact that personal data is rendered at the disposal of a public authority for the purposes of countering tax fraud in itself constitutes a risk.

First, the Court of Justice has clarified that the making the list in question constitutes the processing of personal data within the meaning of the Directive and therefore falls within the scope of that directive. The Court of Justice has then pointed out that personal data may be lawfully processed "if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority."[130] According to the Court of Justice, the collection of taxes and the fight against tax fraud, for which the disputed list is established, must be regarded as tasks carried out in the public interest, but emphasizes that it is for the Supreme Court to assess whether the Slovak authorities who made the list, or those authorities addressed in the list, were entitled to do so under Slovak legislation. Moreover, apart from the principle of legality, it is for the Supreme Court to determine whether the establishment of the contested list is necessary for the purpose of collecting taxes and combating tax fraud and whether those objectives cannot be achieved by less restrictive means. It therefore means that EU law does not preclude the processing of personal data by the authorities

128 See Supreme Court of the Slovak Republic, decision no. 1Sžz/15/2014 from August 23, 2018, para. 6.

129 See Court of Justice of European Union, judgment from September 27, 2017, case C-73/16. The first referred question dealt with a possibility of a Member State to make exercise of the effective remedy conditional upon exhaustion of administrative complaints, the third one aimed at the il/legally obtained registration by the applicant and the possibility of a Member State to refuse such an illegally obtained evidence, the last one focused on a hypothetical collision of the relevant rights protection between the ECtHR and the Court of Justice interpretation (this question was declared inadmissible).

130 Compare ibid. para. 117.

of a Member State for the purposes of tax administration and the suppression of tax fraud.[131]

7. Conclusion

Right to privacy has become a challenge in the digital world. Although there are many definitions of digital world in the literature, for the purposes of this chapter, it has been understood as a globally existing sphere within the information environment whose distinctive and unique character is created by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information through interdependent and interconnected networks that use information and communication technologies.[132] This definition precisely defines that even for the operation of the Internet, we need hardware, software, and data. Moreover, it is clear from this definition that cyberspace also depends on several variables because it is not exclusively about the information itself, but also about the way it is transmitted, whether we perceive it in terms of the need for material components or software. In practice, for example, this means that even if we order the goods online, if we want to have them delivered, we not only order it on some technical equipment, but also have it physically delivered to us, and delivery of goods are tied not to cyberspace, but to real space. Even if we order goods online that are not material in nature, e.g., access to databases, someone had to put the data into the system somewhere, and we have access to it through the media also in real time and space. Therefore, it is problematic to perceive the Internet as an exclusively virtual world that could function without rules.

Although Mark Zuckerberg once stated privacy used to be desirable, but today people want to share, are more open,[133] there are still many areas in which individuals want to maintain their privacy. It is their fundamental right, although they might not always realize how easily they can open it to a worldwide auditorium.

This chapter is a contribution presenting and analyzing selected aspects of the Slovak legal framework in relation to the right to privacy protection in the digital age. Selection criteria have considered challenges of the digital world especially in relation to the quick and broad data processing and challenges that are faced by vulnerable groups or in the areas that are considered sensitive. Therefore, children and their right to protection has been analyzed from the point of view of both, perceiving them as victims and on the other side, possible perpetrators. Comparatively, only from the point of view of possible victims, the issue of un/authorized monitoring of

131 Ibid.
132 Kuehl, 2009, p. 28.
133 See https://www.azquotes.com/quote/1370681.

employees has been analyzed. Finally, because of existing international case law, the un/authorized registration of personal data has been analyzed in relation to right to privacy protection.

The Constitution of the Slovak Republic was adopted on September 1, 1992, and that in relation to its Section II, regulating human rights and protecting fundamental freedoms, there has been no relevant amendment. It means that the regulations of the basic legal act of the state were adopted before the Internet era. Nevertheless, interpretation of the most relevant articles of the Constitution about the right to privacy protection—Arts. 16, 19 and 22—have been an operative tool for effective protection of this right also in the digital sphere. It is so also in relation to the Civil Code and personality rights protection. On the other hand, criminal law must have processed some demands regarding *nullum crimen sine lege* principle and therefore, new crimes have been included into the Criminal Code. Nevertheless, as it has been sadly proved by a particular case study, there are still elements that must be amended in the Criminal Code for the state bodies be able to prosecute non-acceptable online behavior in the form of cyberbullying. Furthermore, as for criminal procedure, existing rules have been adapted to the requirements and specificities of the digital world. To conclude, as for Slovakia in general, traditional means of the right to privacy protection are a preferred tool to deal with challenges of the digital era. However, the area of criminal law is different. Therefore, because of the rule of law, the adoption of a definition of cyberbullying is recommended to be amended *in futuro* so that its criminalization did not depend on the consent of an individual whose audio or audio-visual recording of personal presentation was unjustifiably published or made available to a third party.

It is submitted that since as for the application of legal rules, it has been strictly observed that the basic constitutional principle is to be pursued—that state bodies may act solely based on the Constitution, within its scope, and their actions shall be governed by procedures laid down by law; on the contrary, everyone may do what is not forbidden by a law and no one may be forced to do what the law does not enjoin.[134] It has been proved, as Bill Gates declared, that historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules—not just for governments but for private companies.[135] Finally, it is true that it was difficult to find information. Nevertheless, today, it is difficult to choose among it. One could therefore add that it is important to be aware and respectful of the rules by private individuals as well since you never know to whom you are opening the door to your privacy.

134 Art. 2 of the Constitution of the Slovak Republic
135 See https://www.azquotes.com/quote/1370681.

Bibliography

BROWNLIE, I. (2013) *Princípy medzinárodného verejného práva*. Bratislava: Eurokódex, s. r. o. a Paneurópska vysoká škola.

DRGONEC, J. (2013) *Sloboda prejavu a sloboda po prejave*. Šamorín: Heuréka.

GARAOVÁ, L. (2020) 'Slovakia' in RIJPMA, J.J. (ed.) *The new EU data protection regime*: setting global standards for the right to personal data protection. Hague: Elevent International Publishing, pp. 525–542.

KUEHL, D.T. (2009) 'From Cyberspace to Cyberpower: Defining the Problem' in: KRAMER, F. D., STARR, S., WENTZ, L. K. (eds.): *Cyberpower and National Security*. Washington D C: National Defense University Press, pp. 24–42.

KURUCOVÁ, Z. (2018) 'Aktivity digitálnych domorodcov na sociálnych sieťach', *Media journal,* 6(2), pp. 127–135.

OROSZ, L., SVÁK, J. (eds.) (2021) *Ústava Slovenskej republiky – komentár. Zväzok I.* Bratislava: Wolters Kluwer.

STEINBERG, S.B. (2017) 'Sharenting: Children´s Privacy in the Age of Social Media', *Emory Law Journal*, 66(839), pp. 839–884.

ŠTEVČEK, M., DULAK, A., BAJÁNKOVÁ, J., FEČÍK, M., SEDLAČKO, F., TOMAŠOVIČ, M. (eds.) (2015) *Občiansky zákonník I., II. § 1–880. Komentár.* Praha: C. H. Beck.

STUART, A.H. (2014) 'Google Search Results: Buried If Not Forgotten', *North Carolina Journal of Law and Technology*, 15(3), pp. 463–517 [Online]. Available at: https://doi.org/10.2139/ssrn.2343398 (Accessed: 11 October 2022).

VRŠANSKÝ, P., VALUCH, J. (eds.) (2016) *Medzinárodné právo verejné. Osobitná časť*. Bratislava: Wolters Kluwer.