Chapter VII

The Right to Privacy in the Digital Age in the Czech Republic

David Sehnálek

1. Introduction

This chapter aims to introduce the issue of the protection of the right to privacy in Czech law. The starting point is the regulation of the right to privacy at the constitutional level, which I will follow with a description and analysis of the regulation in the most important Czech statutes that regulate the issue of privacy protection. With necessary exceptions, I will not address the GDPR[1] as I aim to introduce the foreign expert to those areas of Czech law that concern privacy protection but have not yet been affected by unification tendencies at the level of EU law.[2]

The content of this chapter is adapted to this objective, as it provides primarily an overview of the Czech legislation the descriptive method is the prevailing method, and the chapter has a format of a national report.

To achieve the aim of the chapter, I will analyze the right to privacy in a narrow sense, focusing only on those issues that are related to modern digital technologies and their impact on privacy protection.

1 In Czech legal science, the issue of privacy protection in the context of the GDPR is addressed by a number of authors, primarily by Jakub Míšek, and I therefore refer to his work; Míšek, 2017, pp. 331–346; Míšek, 2020; Míšek, Kasl, and Loutocký, 2020, pp. 289–293; Míšek and Bartoš, 2020, pp. 145–174; Míšek, 2014a, pp. 69–84; Míšek, 2014b, pp. 3–74; Míšek, 2014c, pp. 227–229.

2 In the Czech Republic, the GDPR has been supplemented and implemented by Act No. 110/2019 Coll., the Act on the Processing of Personal Data. This act will also not be the subject of examination in this chapter.

David Sehnálek (2023) The Right to Privacy in the Digital Age in the Czech Republic. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 235–272. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_7

Since an understanding of the legislation is not possible without considering the case law, as it is the case law that provides the comprehensive knowledge, I explain and demonstrate the issue using the case law of the Czech Constitutional Court and the Supreme Court. Both courts also work with the case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU). I will not reflect on the case law of these institutions as it goes beyond the purely national scope of the issue.[3]

The first five sections are devoted to the general issues of the right to privacy in Czech law, on the structure, wording, values, and system. Subsequent chapters are more specific and problem oriented. Here, I have chosen areas where there is case law of Czech courts that is directly related to the issue—my aim is to present law in action and not just the law in statutes, commentaries, and scientific articles. One of the starting hypotheses of this publication could be "privacy protection is regulated in the same way in all the countries concerned." The answer to this question can then be provided either by simply comparing the texts of constitutions and statutes, which are likely to be very similar. However, the approaches taken by individual national courts to interpreting these provisions may differ quite significantly. It therefore makes sense to present not only the text of the legislation but also how it has been interpreted and applied by the courts. The chosen areas then reflect those problems that have been addressed by the Czech courts.

2. Overview and systematics of the regulation of the right to privacy at the constitutional level

The current Czech constitutional legislation on privacy protection was adopted in connection with the division of the former federal Czechoslovak Republic. It is contained in several articles of the Czech Charter of Fundamental Rights and Freedoms of the Czech Republic (Czech Charter). The international and EU regulation on this issue is significant and present in the Czech judicial practice. The influence of the German Constitutional Court is also not negligible. Nevertheless, these external sources will not be addressed as they fall out of the scope of the research.

The regulation of privacy protection in the Czech Charter is fragmented and, therefore, quite complicated. The general protection of this right is ensured by Art. 7(1) of the Charter: "The inviolability of the person and his privacy is guaranteed. It may be restricted only in cases provided for by law." The very essence of the right to privacy protection is addressed in Art. 10(1) of the Czech Charter: "1. Everyone has the right to have his human dignity, personal honor, reputation, and

3 In Czech legal science the case law of the ECtHR and subsequent related case law of the Constitutional Court addressed in publication Bónová, 2022, pp. 157–225.

name preserved. 2. Everyone has the right to protection from unwarranted interference with his private and family life. 3. Everyone has the right to protection against the unauthorized collection, disclosure, or another misuse of personal data." Partial protection of privacy is ensured by Art. 12 of the Charter, which states that a person's dwelling is inviolable. Art. 13 of the Czech Charter states that no one may violate the confidentiality of letters or the confidentiality of other papers or records. In a broader sense, the provisions that ensure privacy protection may also include Art. 15 of the Czech Charter, which guarantees freedom of thought, conscience, and religion.

This fragmented concept of privacy protection in Czech law results from political influences in the legislative process. The original draft of the Czech Charter did not include privacy protection at all. It only guaranteed personal inviolability. Subsequently, Art. 7 of the Czech Charter added that the person's right to privacy would also be guaranteed. In parallel, it was also proposed to add to Art. 10(2) of the Charter the protection of private and family life, with the addition of Art. 7 of the Czech Charter being removed. However, the removal did not take place, the reason being the concern that "if the article on the inviolability of privacy is not there, it becomes very questionable what constitutes an unwarranted interference with private and family life within the meaning of the newly adopted Art. 10(2) of the Czech Charter."[4]

Consequently, the legal relationship between the various provisions of the Czech Charter remains unclear. In Prof. Filip's[5] opinion, Art. 7(1) of the Czech Charter is *lex generalis* to the other provisions of the Czech Charter.[6] These provisions contain some specific guarantees; they do not form an exhaustive list but only a regulation of those rights most frequently violated in the past.[7] This approach reflects the legislature's intention and is also supported by the decision-making of the constitutional court in some of its decisions.[8]

There is also a second possible approach to the systematics of the regulation of the right to privacy in the Czech Constitution. According to this approach, Art. 7(1) of the Czech Charter applies only to the *physical and mental integrity of the person*. Therefore, it is not a general clause but a particular and substantively limited provision. The right to privacy is primarily protected in Art. 10 of the Czech Charter. As a result, the two provisions overlap in the case of the processing of personal data obtained through interference with physical and mental integrity, e.g., genetic information, results of a chemical analysis of blood, etc.,[9] as not Art. 7, but also the Art. 10 deals with this issue in its third section. This approach is also supported by

4 Langášek, 2012, p. 186.
5 Prof. Filip is a constitutional lawyer and a judge of the Constitutional Court.
6 Filip, 2011, p. 14.
7 Molek, 2017, p. 295.
8 II.ÚS 770/06.
9 Langášek, 2012, p. 187.

the case law of the Constitutional Court[10] and seems to prevail, even if it does not correspond to the original intention of the legislature. However, it is supported by the system of the Czech Charter, which ranks fundamental rights according to their importance.[11]

The recent decision of the Constitutional Court concerning collecting biological DNA samples has shed light on the relationship between the two provisions of the LZPS.[12] It shows that Art. 7(1) of the Czech Charter indeed protects only the physical and mental integrity of a person. It, therefore, protects privacy in the narrow sense. Art. 10 protects privacy in a broader sense, i.e., against unwarranted interference with private life and against the unauthorized collection, disclosure, or another misuse of personal data, the so-called right to informational self-determination. The Constitutional Court, therefore, favored the first approach.

The Constitutional Court further emphasizes a holistic approach to the issue of privacy protection:

> When interpreting the individual fundamental rights, which are a representation of the right to privacy in its various dimensions as set out in the Charter, it is necessary to respect the purpose of the generally understood and dynamically evolving right to privacy as such, or to consider the right to private life in its contemporary integrity.[13]

Unsurprisingly, the Czech Charter does not give a legal definition of privacy nor defines the right to privacy. Of little to no importance is the fact that Art. 10 of the Czech Charter does not use the term "*right to privacy*," as it refers to the "*right to private (and family) life*."[14]

The Constitutional Court takes a dynamic approach to the content of this right. In its decision II. ÚS 517/99, the Constitutional Court stated:

> The right to protection of personal privacy is the right of a natural person to decide at his or her own discretion whether, or to what extent and in what manner, the facts of his or her personal privacy should be disclosed to other subjects, and at the same time to defend (resist) against unjustified interference in this sphere by other persons. The overemphasis on the positive component of the right to protection of private life leads to an inadequate narrowing of protection to the mere fact that the facts of a natural person's private life should not be disclosed to the public without his or her consent or without reason recognized by law, so that the integrity of the inner sphere, which is essential for the favorable development of the personality, is not undermined. The Constitutional Court does not share this narrow conception

10 IV. ÚS 774/18.
11 Nechvátalová, 2021, p. 225.
12 Pl. ÚS 7/18.
13 Pl. ÚS 24/10.
14 Inspiration was most likely drawn from the text of the European Convention on Human Rights.

> since respect for private life must include, to some extent, the right to form and develop relationships with other human beings. Respect for private life so conceived involves an obligation on the part of the State to act in a way that enables those relationships to develop normally.[15]

Based on this approach to the protection of private life, "the Constitutional Court extended privacy protection to the area of modern technology."[16] This extension happened in a dispute concerning the possibility of exemption from court fees in the case of an indigent person—a disabled retiree who, in the opinion of the general court, was paying excessive Internet fees and therefore had the money to pay the court fees. More precisely, she would have had it if she had not spent it on the Internet. The Constitutional Court disagreed with this approach, stating that

> in assessing the customary or justified nature of the expenditure, objective factors must also be considered; these include, inter alia, technological developments (e.g., mobile phones, the Internet) and the related changes in the methods of communication, obtaining information, dealing with the authorities, association, etc., or the development of technologies through which the individual's right to personal development, relations with other people and the outside world, i.e., the right to private life, is realized.[17]

This approach is an example of the evolutionary approach to the concept of the right to privacy in the Czech Charter and the related case law of the Constitutional Court. The Constitutional Court based its solution on the fact that "in interpreting the various fundamental rights, which are captures of the right to privacy in its various dimensions as set out in the Charter, it is necessary to respect the purpose of the generally understood and dynamically evolving right to privacy as such, or to consider the right to privacy in its contemporary totality." However, this approach must be carefully balanced by resistance to change.[18] Indeed, the driver of change should not primarily be the courts but the legislature.[19] Unfortunately, in information technology, the latter may find it challenging to keep up.

The absence of specific definitions, the general concept of this right in the Czech Charter,[20] and the dynamic approach to its text, has undeniable advantages. Indeed,

15 II ÚS 517/99.
16 Molek, 2017, p. 295.
17 Pl. ÚS 24/10.
18 Kokeš, 2012, p. 331.
19 In the decision Pl. ÚS 45/17, the Constitutional Court emphasizes the legislature's obligation to follow current events.
20 Former constitutional judge Eliška Wagnerová understands the right to privacy to serve, "along with the right to autonomy of the will, as general, overarching clauses that ensure "limitless" protection of liberty as a right even in cases not covered by specific fundamental rights." Wagnerová, 2012, p. 278.

there is no need for legislative changes at the level of constitutional law, despite the rapid development of technology. The evolution of legislation is taking place at the sub-constitutional level. At the same time, the Czech Charter provides ample scope for reflecting these changes through interpretation. The negative consequence, however, is that the shaping of the content of the right to privacy at the highest constitutional level involves a small number of unelected people—the judges of the Constitutional Court, who themselves have different views on how things should be dealt with.

Of relevance to this study is the part of the right to privacy related to *informational self-determination*. In the Czech legal system, it is regulated in Art. 10(3) of the Czech Charter and implies the possibility for an individual to make decisions about him- or herself.[21] However, the problem with modern technologies is that they are attractive to their users, easily accessible, and yet difficult to understand. One may therefore find oneself in the position of a boiling frog. Indeed, the gradual loss of privacy because of "paying with private data" in cyberspace is not apparent. Therefore, an individual has *de iure* the right to informational self-determination, but *de facto* is unable to appreciate and take advantage of this right. He may not be aware of the extent of the data transmitted, nor of the danger he may face.

It has been stated above that the Constitutional Court emphasizes the importance of the Internet and other technologies and sees them as part of the space for individual self-realization. However, this carries the risk of losing one's privacy to a massive, previously unthinkable extent. We are sharing our sensitive data with other individuals, they collect them typically for commercial reasons, and they do so usually in accordance with the law. An equally common motive for intrusion into one's privacy is to enrich oneself through illegal activity. Similarly, states use modern technologies to limit an individual's privacy. The reasons may vary from security (prevention and punishment of crime, prevention of property damage and conflicts—typically by monitoring public spaces or using cameras in common areas of houses, data retention[22]), economic (the much-discussed introduction of EET,[23] operation of electronic vignettes, value-added tax reporting[24]) or practical (introduction of electronic health books or e-prescriptions, registration) or tracing infected persons during the COVID-19 pandemic.

In this view, privacy interests conflict with prima facie countervailing security, commercial and other interests. It might therefore appear at first sight that, as a legislature or a judge, we must choose between protecting one value or the other as both are not possible at the same time. But this view would not be correct. Indeed, by setting up appropriate oversight and regulation, both can be achieved at the same time.[25]

21 Pl. ÚS 24/10.
22 Pl. ÚS 24/10 and Pl. ÚS 45/17.
23 Pl. ÚS 26/16.
24 Pl. ÚS 32/15.
25 Solove, 2011, p. 2. https://ssrn.com/abstract=1827982 (Accessed: 22 June 2022).

As the right to privacy is not absolute, the law can limit it.[26] The trend of developing and shaping the right to privacy in the Czech Republic is well reflected in the Data Retention II decision. In it, the Constitutional Court states:

> Along with the growing threat of terrorist attacks, a logical trend has developed to strengthen the powers and tools of public investigative authorities at the expense of maintaining the existing standard of fundamental rights of individuals. However, this trend is gradually changing over time, and also as a result of decisions of the Constitutional Courts, the ECtHR, or the CJEU, political representations are beginning to understand the need to find a balance whereby States can effectively and efficiently fulfill their positive obligations without interfering more than is strictly necessary in a democratic society with the fundamental rights of individuals, in this context, in particular, the right to privacy and informational self-determination under Art. 10(2), (3) and Art. 13 of the Charter. The change in the trend towards strengthening the protection of personal data, or rather redressing the lost balance, is demonstrated, inter alia, by the adoption of the GDPR or the preparation of the adoption of the so-called e-privacy Regulation, regulating the area of privacy and electronic communications instead of the existing directive of the same name. The rapid development of information technology cannot be stopped or slowed down by any legislation; the reach of the Internet and other networks enabling electronic communication is not limited to national borders but is a global phenomenon, a worldwide phenomenon that national legislatures deal with it in different and difficult ways. It is necessary to deal with the fact that a plethora of different data (metadata) is being generated by the active involvement of individuals, and the risk of its misuse is increasing exponentially—the means of protecting personal data must be adapted to this. The Constitutional Court has concluded that in the conditions of today's information society, in which the average individual uses electronic communication services at almost every step and voluntarily accepts that quantum amounts of data are stored about him, it would be unwise to tolerate a situation in which service providers have users' data, and the state apparatus (in justified cases) does not. The blanket retention of traffic and location data represents an effort by the State to keep pace in the information society and have effective tools to carry out its tasks—here in particular in security of the State and its citizens.[27]

The decision shows a certain degree of *resignation to a high level of privacy protection.* This is contrary to trends at the EU level. It is being done so just in favor of the public authorities, for purely factual reasons, and moreover, for reasons caused by the private sphere. At the same time, the factual situation is perhaps overemphasizing the question of the extent to which the storage of individual data is voluntary. Regarding

26 However, even the law cannot exceed the limits set by the Constitution and the Czech Charter. Art. 7 of the LZPS prohibits torture or cruel, inhuman, or degrading treatment or punishment.

27 Pl. ÚS 45/17 34.

trends at the EU level, the Constitutional Court monitors and respects the external legal environment. The standards of privacy protection contained in the EU Charter of Fundamental Rights and the European Convention, and consequently also in the case law of the ECHR and the CJEU, are routinely used and cited in its decisions.

3. Overview and systematics of the regulation of the right to privacy at the sub-constitutional level

At the sub-constitutional level, the right to privacy is regulated in private law primarily by Act No. 89/2012 Coll., the Civil Code. This statute regulates in Arts. 81 to 91 the protection against the dissemination of likenesses and the protection against invasion of privacy in accordance with the Czech Charter.[28] Protection is thus granted only to natural persons. At the same time, the Civil Code contains provisions on exceptions—official licenses, based on which interference with this right is permissible.

The protection of the privacy of legal persons is provided for in Art. 135 of the Civil Code.[29] Case law on this provision regarding the privacy of legal persons does not yet exist.[30] At the same time, Prof. Dvořák, author of the commentary on this provision, asks the question of how the privacy of a legal entity can be interfered with at all if it is a simple fiction. He also argues that the protection of privacy in this provision is a legislative technical error, something that the legislature did not intend to regulate at all.[31] Therefore, it can be concluded that although there is a legislative space for the protection of the privacy of a legal person, it has not yet been filled by practice and legal theory does not yet know how to deal with it.[32] Within the sphere of civil law, specific regulation of the right to privacy is secured by the Act No. 262/2006 Coll., the Labor Code in labor legal relations.

In administrative law, the protection of the right to privacy is ensured by Act No. 127/2005 Coll. on electronic communications, as amended, Act No. 181/2014 Coll. on cybersecurity, Decree No. 82/2018 Coll. on cybersecurity, and several other

28 The value significance of the right to privacy is generally emphasized by its mention in Art. 3, para. 2 of the CC.

29 This provision states: "(1) A legal person which has been affected by having its right to a name disputed or which has suffered harm due to unlawful interference with that right, or which is under threat of such harm, in particular by unauthorized use of the name, may claim that such unlawful interference be refrained from and its consequence remedied. (2) A legal person enjoys the same protection against anyone who, without a lawful reason, interferes with its reputation or privacy, unless for artistic or scientific purposes or for print, radio, television or similar coverage; however, neither such an interference may be in conflict with the legitimate interests of the legal person."

30 More precisely, I am not aware of its existence, and leading commentaries do not mention it either.

31 Dvořák, 2014, p. 461.

32 Lasák in another Czech commentary does not discuss nor question the privacy of legal persons at all. Lasák, 2014, p. 713.

regulations address the right to privacy to some extent. In the healthcare sector, privacy is regulated by the requirement of confidentiality in relation to healthcare services. This regulation is contained in Act No. 372/2011 Coll. on Health Services and Conditions of their Provision.

In criminal law, the protection of privacy is provided for in Act No. 141/1961 Coll., the Criminal Procedure Act, in Articles 180 to 184, which regulates Criminal Offences against Rights for Protection of Personality, Privacy, and Secrecy of Correspondence. Specifically, the following offenses are regulated: Illicit Disposal with Personal Data,[33] Infringement of Rights of Another,[34] Breach of Secrecy of Correspondence,[35] Breach of Confidentiality of Files and other Private Documents,[36] and Defamation.[37] The Criminal Law further protects against cyberstalking.[38]

The two procedural rules governing evidence are also relevant to the protection of privacy. In the area of civil law, evidence taking is regulated by Act No. 99/1963 Coll., the Code of Civil Procedure, which does not contain any special provisions specifically addressing privacy protection in the context of digital technologies. In the area of criminal law, the issue is regulated by Act No. 141/1961 Coll. on Criminal Procedure. This Act regulates the protection of privacy both through general institutes and through newly adopted provisions that consider modern technologies. Specific provisions of this law regulate the interception and recording of telecommunications[39] and further surveillance of persons and items during which any audio, visual or other records shall be made.[40]

4. Privacy and modern technologies in the civil law of the Czech Republic – General remarks

The Civil Code enshrines the protection of privacy in its Art. 3, according to which

> Private law protects the dignity and freedom of an individual and his natural right to pursue his own happiness and the happiness of his family or people close to him in a way that does not unreasonably harm others. (2) Private law rests in particular on

33 Art. 180 of the Criminal Code.
34 Art. 181 of the Criminal Code.
35 Art. 182 of the Criminal Code.
36 Art. 183 of the Criminal Code.
37 Art. 184 of the Criminal Code.
38 Art. 354 of the Criminal Code.
39 Art. 88 of the Code of Criminal Procedure.
40 Art. 158d of the Code of Criminal Procedure.

> the principles that (a) everyone has the right to the protection of his life and health, as well as of his liberty, honor, dignity, and privacy.[41]

From a systematic point of view, the quoted provision is, as far as the right to privacy is concerned, a simple repetition of what is already contained in the Charter. The cited Regulation contained in the Civil Code, therefore, does not constitute any added value since it does not extend or further specify the general constitutional framework in any way but merely repeats it.[42] The quoted provision elevates the protection of privacy to a *principle*, but in reality, the protection of privacy is a *value* and the intention of its protection as *a policy*.[43] The significance of the quoted provision can therefore be seen only in the fact that it emphasizes the legislature's interest in protecting this value and presupposes its horizontal application in Czech civil law by the courts and the addressees of this legislation.

The protection of privacy is ensured in Czech private law by means of the general clause of protection of personality rights and the specific provisions of the Civil Code. According to the general clause contained in Art. 81 of the Civil Code, "The personality of a person, including all his natural rights, is protected. Everyone is obliged to respect a person's free decision to live according to his own." This general provision is followed in the same clause by a demonstrative enumeration of human values, according to which "the life and dignity of the human being, his health and right to live in a favorable environment, his dignity, honor, privacy and his expressions of his personal nature shall, in particular, enjoy protection." Human privacy is specific among these values in that a violation of any other value that is protected by the cited provision will also result in an invasion of privacy.[44]

The regulation of privacy protection is further specified by the Civil Code in the provisions of Art. 84 to Art. 90. These provisions build on the general clause and are included in subsection 2 of the Civil Code, entitled *Likeness and Privacy*. The two interrelated rights are therefore regulated together. The protection of privacy is primarily provided for in Art. 86 of the Civil code. According to this provision,

> no person shall invade the privacy of another unless he has a lawful reason to do so. In particular, one may not, without a person's consent, invade his or her private premises, monitor his or her private life or make audio or visual recordings of it, or use such or other recordings made of a person's private life by a third party, or disseminate such recordings of his or her private life. Private writings of a personal nature shall be protected to the same extent.

41 Art. 3 of the Civil Code.
42 See Pelikán and Pelikánová, 2014, p. 25.
43 Ibid.
44 Ondřejová, 2016, p. 199.

It is clear from the text of this provision that the right to privacy has *erga omnes* effect. At the same time, this right may be limited by law and is therefore not absolute. The following provisions of the Civil Code provide for limitations (so-called *statutory licenses*). These permissible limitations overlap with those provided for in the data protection regulations.[45] Restrictions are possible where *consent is given* to interfere with the right to privacy,[46] in the case of an official license, i.e., to protect one's own rights or the rights of a third party,[47] and for scientific or artistic purposes and for press, radio, television, or similar reporting.[48]

Of course, the legislation does not preclude the granting of consent to the interference with the right to privacy (principle of autonomy). This possibility is often used in cyberspace. Personal data is commonly used as a form of consideration for services provided or as a prerequisite for a discount on the normal price of services or goods.

Consent should be given in advance, knowingly and transparently. It may be hard to meet these requirements in cyberspace for two reasons. First, in an electronic environment, it is relatively easy to "hide" consent among other provisions, thereby making it "invisible." Second, people often do not carefully read the contracts they enter online. While the first practice is legally solvable, especially in the case of consumers, the second situation does not have an easy solution. On the other hand, rights belong to the vigilante, and the law should not be overly paternalistic.

It follows from the above that consent to an interference with the right to privacy is necessary in some cases under the Civil Code. Consent to the processing of personal data is also foreseen and required by the GDPR. There is to some extent an overlap between privacy and data protection. In case of such overlap, only one consent is fully sufficient. The parameters of consent are not explicitly defined by the Civil Code, therefore the general and rather lenient rules governing legal conduct apply. The GDPR, on the other hand, defines the scope, form, and other elements of consent quite precisely. In view of this fact, I therefore conclude that in the case of consent granted based on the GDPR which meets the strict criteria set by this act, the conditions required by the Civil Code are also fulfilled and no other action is needed.

Any ill-considered or unintended consent is legally solvable. It is also possible to change your mind and reconsider previously granted consent. The provision of Art. 87 of the Civil Code allows for the *unilateral withdrawal of consent already given*. This possibility is even available if the consent has been granted for a fixed period. The provision is mandatory. The possibility of withdrawing consent already granted cannot, therefore, be excluded even by mutual agreement of the parties.

Withdrawal of the consent granted for a fixed period may constitute a serious interference with the right of the other party. The Civil Code, therefore, provides

45 Nonneman, 2012, p. 508.
46 Art. 87 of the Civil Code.
47 Art. 88 of the Civil Code.
48 Art. 89 of the Civil Code.

that if this is done "without a material change in circumstances or other reasonable cause, the person revoking the consent shall compensate the person to whom the consent was given for the damage resulting therefrom."[49] This opens the way for compensation in the case where consent is tied to a certain consideration, this is consumed, and consent is subsequently revoked on purpose.

The possibility of withdrawing consent looks easy and unproblematic at first sight. Legally, it is. In practice, however, misunderstandings arise. I can demonstrate such a problem by the hoaxes that periodically appear and spread on Facebook.[50] The gist of one of them (including various sub-variants) is that the persons whose privacy is at stake must share a text in which they explicitly do not give Facebook their consent to use what they themselves have previously shared. In this case, however, consent is a condition of the use of the service as by creating a Facebook account, and a customer enters into a contract which is the legal basis for personal data processing. Therefore, withdrawal of consent cannot be made unilaterally in a situation where the service is still being used. To make such a change, it would also be necessary to change the content of the contract, i.e., to renegotiate it with Meta, the company that operates Facebook, which is not very likely.[51] It appears that many of the recipients of the legislation do not understand how the law works (see the references to the Berne Convention in the hoax quoted above), nor do they understand the basic concepts. Sharing such hoaxes, on the other hand, reveals a great deal about the people who share them.

Of legal significance is the question of how to proceed in situations where consent to interference with the right to privacy is lacking. Modern technology makes it possible, to a degree previously unthinkable, to make a video or audio recordings of people without their knowledge. Given the continuing miniaturization, it is also increasingly unlikely that the making of such recordings will be detected by those being recorded.

49 Art 87, para. 7 of the Civil Code.

50 The text of one of the variants reads, "As of January 3rd, 2015 at 3:30 p.m. Central standard time. I do not give Facebook or any entities associated with Facebook permission to use my pictures, information, or posts, both past and future. By this statement I give notice to Facebook it is strictly forbidden to disclose, copy, distribute or take any other action against me based on this profile is private and confidential information. The violation of privacy can be punished by law (UCC 1-308-11 308-103 and Rome statute). NOTE: Facebook is now a public entity. All members must post a note like this. If you prefer, you can copy and paste this version. If you do not post this statement at least once it will be tactically allowing the use of your photos, as well as information contained in the profile status updates. DO NOT SHARE you MUST copy and paste this… I will leave a comment so it will be easier to copy and paste!!!" [Online] Available at: https://www.lupa.cz/clanky/facebookovy-hoax-s-pravy-k-prispevkum-se-vraci/ (Accessed: 07 September 2022).

51 For the sake of completeness, I would like to add that Meta is thus entitled, pursuant to Art. 6, para. 1b of the GDPR, to process only the personal data necessary for the performance of a contract. The customer's consent will nevertheless be required for further processing and further services. However, the eventual revocation of such consent cannot technically be done in the manner suggested in the hoax. The revocation was not, at least under Czech law, properly served the other party.

From a practical point of view, the significance of interference with another privacy is that it may enable things to be proved that would otherwise be impossible to prove. One is often more likely to say things in private that one would not say in public, and one is also more likely to speak plainly, truthfully, and openly about what one thinks. In such a situation, the rules in procedural law that courts should decide based on truth[52] collide with the substantive rules protecting privacy. Solutions to this problem in Czech law will be introduced below.

5. Instruments of enforcement of the right to privacy in Czech private law

Under Czech law, the right to privacy is not *time-barred*. However, this does not apply to rights to compensation for harm caused to these rights.[53] The general statute of limitations in Czech law is three years, so it is necessary to bring an action to court within this period.[54] The person concerned has the right to claim that the unlawful interference is refrained from or its consequences remedied.[55]

The invasion of an individual's privacy by modern digital technologies can have far-reaching and difficult-to-remedy consequences. The publication of defamatory text, photographs, videos, or other recordings can affect the psyche of a person, especially a young, developing person, in a severe and irreversible way. The legislation, therefore, provides for the possibility that even *non-pecuniary harm* caused in this way is compensated by appropriate satisfaction. Satisfaction must be provided in money unless real and sufficiently effective satisfaction for the harm incurred can provide for satisfaction otherwise.[56] It follows from the above that monetary compensation is only a secondary instrument of compensation for the injured person in the Czech law. The primary one would be, for example, a public apology, or a withdrawal of problematic information. However, such a solution will not always be an option either. Furthermore, the Czech Civil Code also explicitly provides for the possibility for the injured party to claim *compensation for the mental distress caused*.[57]

As the act of interfering with an individual's privacy may also have an impact on other persons (e.g., the parents of a child who has been affected by interference

52 Czech civil litigation is based on the principle of formal truth. The principle of substantive truth, and thus the accurate determination of the facts, is important in civil non-contentious proceedings and in the area of administrative and criminal proceedings.
53 Art. 612 of the Civil Code.
54 Art. 629, para. 1 of the Civil Code.
55 Art. 82 of the Civil Code.
56 Art. 2951, para. 2 of the Civil Code.
57 Art. 2956 of the Civil Code.

with privacy on the Internet), the Czech law also provides for the possibility of also compensating these third persons.[58]

Finally, Czech law also protects against someone else's enrichment by interfering with one's right to privacy. In such a case, the injured party may claim: 1) that an enriched person who did not act in good faith makes restitution of the entire enrichment he acquired, and 2) that he also compensates for the revenue which the impoverished person would have gained.[59] Alternatively, as compensation for the unlawful disposal of the values related to his personality rights, the impoverished person may demand twice the remuneration usual for the consent to such disposal.[60]

6. Privacy protection and modern technologies in Czech civil procedural law—Cases on the right to privacy and the right to a fair trial

The Czech procedural rules are set very generally, as they do not explicitly regulate the issue of electronic evidence; in my opinion, that is a good approach from the point of view of modern digital technology because the legislation is in line with the principle of technological neutrality. According to Art. 125 of the Code of Civil Procedure, "all means by which the state of the case can be established may be used as evidence." This creates an apparent conflict, as the Civil Code sets certain conditions should the interference with privacy be admissible, and these conditions may not be met (for example the consent is missing, or there is no official statutory license), whereas under the Code of Civil Procedure, no precondition in the form of the consent of the person concerned is required.

The Czech civil courts have dealt with this problem pragmatically in two ways. First, by interpretation of the terms "privacy" and "expressions of a personal nature." Second, the problem has been addressed by balancing the various interests involved. It must be stressed that the resolution of individual situations is ambiguous and the conclusions of the various courts, as well as their legal reasoning, often differ widely.

58 However, the conditions are set very strictly. See Art. 2971 of the Civil Code: "If justified by special circumstances under which the tortfeasor caused harm by an unlawful act, including, without limitation, by breaching an important legal duty due to gross negligence, or by causing harm intentionally out of a desire to destroy, hurt or for other especially reprehensible motives, the tortfeasor shall provide compensation for the non-pecuniary harm to everyone who legitimately perceives the harm as a personal misfortune which cannot be undone otherwise."

59 Art. 3004, para. 1 of the Civil Code.

60 Art. 3004, para. 2 of the Civil Code.

An example of the first solution is a situation that arose in a dispute between the partners of a commercial company. One of the partners made an audio recording of a meeting, which was subsequently used as evidence in court proceedings. In this case, both the first instance court as well as the court of appeal concluded that the taking of the recording without consent violated the individual's right to protection of personality, but the provisions of the procedural rules that all means of establishing the situation may be used as evidence in proceedings allow such evidence to be taken in proceedings before the competent public authority, as they create an official statutory license. However, the Supreme Court did not accept this reasoning and came up with a different solution. It noted that the Civil Code, in the provisions at issue, provides

> protection only for those expressions of natural persons which are personal in nature. Therefore, as a rule, speeches that occur in the exercise of a profession, in commercial or public activities do not have a personal character. The audio recording admitted in evidence by the courts in the present case is a recording of the proceedings of the shareholders of a commercial company, and this recording concerns solely the company's problems. In such circumstances, therefore, the participants' speeches in the recorded conversation cannot be regarded as being of a personal nature. It follows from the foregoing that making the sound recording in question could not have infringed the personality rights of the parties.[61]

The conclusions contained in this decision have been further elaborated in the case law of the Supreme Court. In the Czech Republic, a new Civil Code came into force in 2014, which expanded the possibilities of limiting the right to privacy. In contrast to the previous regulation, the new Civil Code also allowed the taking or use of an image or a sound or visual recording regarding the exercise and protection of other subjective private rights, generally in proceedings before a public authority and under public law. In a dispute concerning the validity of an employee's dismissal, recordings were used that captured threats made by the employee. The Supreme Court stated,

> a sound or visual recording which relates to a person or his expressions of a personal nature and which was made by a private person without the knowledge of the person recorded may be used as evidence in civil proceedings only where it is intended to lead to the proof of a fact which cannot otherwise be proved (by evidence, which does not interfere with the absolute personality rights of the person concerned), and where the other circumstances of the case lead to the conclusion that the right to protection of the personality of the person concerned cannot be given priority over

61 30 Cdo 64/2004.

> the right to a fair trial of the person who benefits from the use of evidence of an audio or visual recording relating to that person or his or her personal manifestations.[62]

In the present case, however, facts could otherwise be proved according to the Supreme Court. Witnesses were also present at the hearing. Therefore, a recording was not necessary to prove the facts. However, the important issue, in my view, is the quality and credibility of the individual pieces of evidence. Formally, the evidence is equal under Czech law, but in fact, the testimonial value of the recording may exceed that of the witness statement. A recording captures and preserves the course of events in an objective manner. In contrast, witness testimony depends on several subjective factors, including the quality of memory and the ability to reproduce what is heard (and seen).

The Constitutional Court used both methods of justification in a case involving a wrongfully dismissed employee. This employee was formally dismissed out of redundancy. However, the real reason for his dismissal was that he had complained about the company's management to its foreign owner. This was supposed to be evidenced by an audio recording, but it was made without the knowledge of the person being recorded. The Constitutional Court referred to the earlier case law of the Supreme Court (cited above). It stated that the recording was made during work and was therefore not protected in principle as a manifestation of a personal nature. However, if it did contain expressions of a personal nature, the right to a fair trial would still prevail. According to the Constitutional Court,

> in normal circumstances, the arbitrary recording of private conversations without the participants' knowledge is a gross interference with their privacy. In most cases, such a practice, which has the appearance of being insidious, is morally and legally unacceptable, especially if it is motivated by the intention to harm the person being recorded. The Constitutional Court is firmly opposed to the unfair practice of electronic surveillance and covert recording of private and professional meetings, which, as a rule, not only contravenes the law, but also, from a social and ethical point of view, spreads an atmosphere of suspicion, fear, uncertainty, and distrust in society. However, a completely different approach should be taken in cases where the secret recording of an audio recording of a conversation is part of the defense of the victim of a crime against the perpetrator or where it is a way of obtaining legal protection for a significantly weaker party to a significant civil and labor law dispute. The interference with the right to privacy of the person whose speech is recorded is fully justified here by the interest in protecting the weaker party to the legal relationship who is at risk of serious harm (including, for example, loss of employment). The provision of a single or key piece of evidence in this way is analogous to acting under conditions of extreme hardship or self-help leave. In the present case, the admission of the complainant's recording of an interview with NV, one of the

62 21 Cdo 1267/2018.

> intervener's foreign executives, in the proceedings for the annulment of his dismissal is fully consistent with the legitimate aim pursued, which is, as a matter of priority, the protection of employees and the very protective function of labor law vis-à-vis the employee in employment relationships.[63]

It can be deduced from the reasoning of the Supreme Court and the Constitutional Court that the use of evidence interfering with the right to privacy without the consent of the person concerned is an exceptional situation. Firstly, it will be admissible if there is no other way of proving the fact in question, unless the sole purpose of the recording is to harm the person being recorded. This option is always permissible, regardless of the nature of the parties concerned. Secondly, such evidence will be admissible even where there is a possibility of proving the relevant fact by other means. However, this is possible only in exceptional circumstances where the weaker party to the legal relationship in question uses such evidence as a defense. The concept of the weaker party may include not only an employee, but also a consumer, a victim of crime, and presumably the elderly, young children, seriously ill persons, etc. This form of protection, on the other hand, will not be afforded to employers, commercial companies, criminals or the Czech state and its authorities.

The case above concerned a situation, where the protection of privacy was secured primarily by the Civil Code which sets conditions and limits of this protection. On the contrary, a telephone calls between commercial companies (and their employees) falls outside the scope of the privacy protection provided by the Civil Code. Conditions and limits set by this act thus do not apply on such a situation. However, the mechanism for resolving conflicts between the right to a fair trial and the constitutionally protected right to privacy is the same as in cases, where the Civil Code applies. The Constitutional Court did come to this conclusion in a case involving a dispute between two commercial companies. The dispute concerned the admissibility of evidence in the form of a recording of a telephone conversation. The call had been monitored, so the general courts concluded that the recording was not admissible. This was because the company had only consented to monitoring, not storage of the call. On the contrary, the Constitutional Court stated:

> When the right to judicial protection is weighed against the right to privacy, the right enshrined in Art. 36(1) of the Charter must be given priority in this case. It cannot be overlooked that the communication concerned a business case between two business entities and the intervener was aware of the monitoring of the call. The purpose of taking that evidence was precisely to prove that the contract which was the subject of the call had been concluded. Therefore, it cannot be considered that this evidence was intended to interfere with the privacy of any person or to be misused for other purposes. In the view of the Constitutional Court, the taking of evidence of a recorded telephone call, the subject of which was a commercial offer, does not exceed

63 II.ÚS 1774/14.

an unacceptable degree of contextual interference with the fundamental right to privacy. In the opinion of the Constitutional Court, this is sufficient for the applicability of such evidence in court proceedings.

The case concerned a recording made in secret. However, in the course of work, situations may arise where a person is filmed without being able to defend against it. These situations typically arise during professional, commercial, or public activities. For example, a student may record a lecture by his lecturer, a citizen may record a police officer during a raid[64] or a politician during a meeting of a public authority. Similarly, recordings can also be made of persons who, although they do not hold political office and therefore cannot be considered politicians, have made a public speech at a meeting of a public authority.[65] Naturally, only what relates to the performance of *public activities* may be recorded in this way; speeches of a purely private nature relating to family, health, etc., cannot be, in principle, recorded.

7. Privacy protection and modern technologies in Czech law – Unsuccessful justification

While victims of crime may defend themselves against recordings that constitute an invasion to the right to privacy, even this defense has its limits. Such recordings may not be used in an "offensive manner." This problem can be illustrated by a well-known dispute which was covered by Czech media. In this case, a person who was robbed of his laptop used his IT knowledge to his advantage. The truth is, that he was essentially forced to do so by the fact that the Czech Police was unable to find the perpetrator of the theft. The robbed person gained remote access to the laptop and took pictures of the persons using the laptop and posted the pictures on the Internet. They were published together with derogatory nicknames he gave them according to the characteristic use of the laptop ("farmer," "wanker"). However, the persons concerned did not steal the laptop but bought it legally (albeit at a conspicuously low price). The dispute dragged on for many years, the problem being to determine whether the robbed IT specialist had acted legally and, if not, what damages he should compensate the persons concerned for the unwarranted invasion of their privacy. However, there was a clear agreement between the courts that the

64 See the Opinion of the Security Policy Department of the Ministry of Interior on the acquisition of police officers' signs in the performance of their duties.

65 Judgment of the Municipal Court in Prague 8 A 316/2011-47.

publication of photographs on the Internet constituted an infringement of the right to privacy.[66]

Coercive use of data that invades a person's privacy is common. As a rule, however, they infringe personal rights and not directly the privacy of the person concerned. Such behavior was also common in the days before the Internet, Facebook, etc. The Supreme Court has commented on this issue in a case concerning alleged non-payment of rent. This information was published by the property owner in a periodical he published and was presented to the public as a so-called "public criticism."[67]

Public criticism is permissible in the Supreme Court's jurisprudence in certain circumstances. However, it must not be out of proportion to the objective of the criticism. This will be the case, for example, if it implies an intention to disparage or insult the person criticized (so-called intense excess).[68] Similarly, public criticism of a person's conduct is inadmissible if the reasons which justifiably led to the conduct complained of are concealed or obscured from the critic. From this perspective, it was also legally inadmissible to publish information on the rental debt without properly explaining the context.[69]

Public criticism is frequent on social media. It is common for people and companies to post information in pursuit of their own personal gain, but also for the "public good". Indeed, just recently, I noticed on the Facebook pages of two of my friends that they independently shared similar information about a Russian soldier who was supposed to have sent his wife "loot" weighing half a ton from Ukraine. The information was accompanied by a photo of the soldier, his wife, and their family. Sharing such information without any possibility of verifying its veracity is legally problematic considering the above rules. What makes it even more piquant is that one of the sharers is a law school graduate.

Such conduct would be permissible in a situation where a person himself or herself decides to disclose certain information belonging to his or her private sphere, e.g., by posting it on Facebook or Instagram, e.g., to boast. The further sharing of this information, if it has not been altered or consent to disclosure withdrawn, would in principle no longer be subject to privacy protection.

Such conduct may also be permissible should it fall withing the concept of *citizen journalism*. Generalizing the described problem, I conclude that its core lies in the conflict between the right to privacy and the right to freedom of expression. Within

66 Pokorný, 2017, Šmírovaní uživatelé kradeného notebooku si na odškodné počkají. Soud musí případ znovu projednat [Online] Availabe at: https://zpravy.aktualne.cz/domaci/smirovani-uzivatele-kradeneho-notebooku-si-na-odskodne-pocka/r~874defd01f6211e7bc55002590604f2e/ (Accessed: June 22, 2022) and Kočí, 2011, Případ šmírujícího MacBooku — co v Televizních novinách nebylo [Online] https://www.lupa.cz/clanky/pripad-smirujiciho-macbooku-co-v-televiznich-novinach-nebylo/ (Accessed: 22 June 2022).

67 30 Cdo 4613/2007.

68 30 Cdo 2573/2004.

69 30 Cdo 4613/2007.

the framework of freedom of expression, protection is granted to all persons who are active in the field of journalism (the journalistic exception). Journalism is understood very broadly in the case law of the CJEU,[70] so that even the lawyer described above — a graduate of my alma mater — may in each case fulfill the characteristics of a *person active in the field of journalism*. However, the essential difference between the case dealt with by the CJEU lies in the fact that in this case the original source of the information was obtained illegally, the information can be made public in an alternative way, i.e., in a way that ensures the protection of the rights of the persons concerned without reducing the information value. I therefore consider the case of sharing pictures described above to be disproportionate and unlawful. In my opinion, the journalistic exception is rather inapplicable in his case.

8. Privacy of third persons and modern technologies in administrative and court proceedings

Special rules apply to work in the public administration. In administrative law, the possibility of making recordings of the proceedings, and thus also of the official, is not provided for directly by law. Nevertheless, in view of the constitutional principle contained in Art. 2(4) of the Constitution, every citizen may do what is not prohibited by law. No one may be compelled to do what the law may not impose. No law prohibits a party to an administrative procedure from making an audio recording of the course of an oral hearing, and it is irrelevant whether the proceedings is public or private. Therefore, there is no basis for concluding that by making an audio or visual recording of the proceedings a party is grossly disorderly and may be banned from the place of the hearing. This could only occur in a situation where, in accordance with the provisions of Art. 63 of the Act No. 500/2004 Sb. Administrative Procedure Code, taking of a recording would constitute a gross disturbance of the peace.[71]

In court proceedings, the possibility of making a recording is expressly regulated. Provision of Art. 6(3) of Act No. 6/2002 Sb. Courts and Judges Act directly provides that

> visual or audio transmissions and visual recordings may be made during a court hearing only with the prior consent of the president of the chamber or a single judge. Sound recordings may be made with the knowledge of the President of the Chamber or a single judge; the President of the Chamber or a single judge may prohibit the making of such recordings if the way they are made is likely to prejudice the conduct or dignity of the proceedings.

70 See case C-73/07 Satamedia Oy.
71 5 As 37/2009-99.

When making a recording, a situation may arise where the recording captures a person whose privacy is not guaranteed — for example, because he or she is acting within the scope of his or her employment (or business). At the same time, however, the recording may include a third party who is protected. This will be the case, for example, in a public meeting of a city council, where the recording of the meeting will capture both the politician and official as well as the public present.

The Civil Code protects not only privacy, but also the likeness of a person. Therefore, as a result "the depiction of a person's likeness in any way so that his identity can be determined from the depiction is only possible with his consent."[72] The protection is provided for situations where a person's likeness is captured, it is not relevant in what form the capture is made (thus, various technical means may be used, such as photography, film, digital recording, but also painting, graphics, etc.) and, finally, the possibility of determining the identity of a person from the depiction is provided, where the depiction of a person contains a sufficient number of characteristic features of the likeness of a particular person by which he or she can be identified as a unique and unmistakable being.[73]

In the case of recording the proceedings of a court, administrative authority, etc., from the perspective of Czech law, there is in principle no interference with their privacy, but their consent is necessary to capture their image on the recording. The solution is therefore not to record such proceedings at all, or to anonymize the recording by blurring or overlaying a substantial part of the third party's face.

Fortunately, while consent must be given, the law does not specify its obligatory form. In practice, therefore, many situations will be solvable by assuming a person's consent to the capture of his or her likeness when a person knows about the fact that the recording is being made and knowingly enters premises (public or private) that are declared as monitored (in any form — e.g., by an explicit warning or even just by visibly installed cameras, etc.).[74]

9. Privacy policy and audio, visual, or other recordings of an item

Protection against interference with a person's privacy is provided *solely to people*. Therefore, the publication of a photograph or video or audio recording of a thing (a house, a car etc.) will not, by its nature, generally be an invasion of privacy. The Supreme Court came to this conclusion in a case involving the publication of photographs of a house that was accompanied by the surname of the owner of the house.

72 Art. 84 of the Civil Code.
73 Pavlík, 2014, p. 324.
74 Ibid.

The Supreme Court stated that the general rule would be that

> The publication of a photograph of a house does not constitute an unwarranted interference with the personal rights of the owner of the house, namely his right to privacy, because a house is a thing that is perceptible from the outside and therefore does not belong to the sphere of personal privacy, which is the inner intimate sphere of a natural person's life necessary for his self-realization and further development.

At the same time, however, it also stated that such publication may

> possibly be an inherently inadmissible probe into the intimate sphere of a natural person, capable of illegally informing the public about his individual foundation, or focus, direction, etc.—i.e., in general, inadmissibly testifying about the private sphere of a natural person.

The above shows that context always matters. *The whole body of information that is provided and its predictive value in relation to a particular person is therefore essential*. The regulation is general, and it is therefore always for the court to make a specific assessment. This is not a criticism of the legislation; life is varied, and it is therefore not desirable for the legislation to cover every conceivable possibility.

---

10. Invasion of children's privacy by their parents — "Sharenting"

The development of information society services, the various social networks, has facilitated the dissemination of information that falls within the sphere of privacy. It is not usually a problem if one shares information about oneself. Part of our freedom is also the freedom to decide which part of our privacy becomes public.

The problem arises when we share information about another person. Consent can be given *ex post*, even by implied consent. This was the case, for example, with the famous hockey player Jaromír Jágr, whose lover posted a photo on social media after a night spent together.

However, the situation is different when information falling within the sphere of privacy is published by persons who have the right to do so, but which concerns another person who cannot decide for himself or herself. Typically, this will be the case for parents and children ("sharenting") and may also apply to persons deprived of their legal capacity and their guardians. More broadly, this also includes the activities of schools and nurseries that publicly share what is happening inside their institution, either by photograph or video.

Invasion of a child's privacy can occur in different ways in an online environment. Parents can use their child's identity to create a social networking profile, which they manage themselves. They can also share information, photos, or videos relating to their child through their own profile. From a privacy perspective, there is no practical difference between the two situations. Leaving aside the security risks of such behavior, as well as the moral considerations (including the impact that sharing information in the environment of the "eternal" Internet may have on their child one day in the future), there remains the problem of the permissibility of such behavior.

Czech courts have not yet resolved a dispute between a parent and a child concerning the disclosure of information about the child's life. At the same time, no specific legislation has been adopted to address this issue. Therefore, only the general legislation regulating the position of parents in the upbringing of a child is applicable. This regulation is, nevertheless, according to my opinion sufficient.

The issue is in the Czech law regulated primarily by the provision of Art. 858 of the Civil Code, according to which:

> Parental responsibility includes rights and duties of parents consisting in caring for the child, including, without limitation, care for his health, his physical, emotional, intellectual and moral development, the protection of the child, maintaining personal contact with the child, ensuring his upbringing and education, determining the place of his residence, representing him and administering his assets and liabilities; it is created upon the child's birth and extinguished upon the child acquiring full legal capacity. The duration and extent of parental responsibility may only be changed by a court.[75]

This regulation is followed by Art. 875, which implements the international legal obligations of the Czech Republic, and according to which "Parents exercise parental responsibility in the best interests of the child." This provision further provides that

> Before making a decision that affects the interests of the child, parents shall inform the child of everything that is necessary for the child to form his own opinion on a given matter and communicate it to the parents; this does not apply if the child is unable to properly receive the message or form his own opinion or communicate it to his parents. Parents shall pay due attention to the child's opinion and take the child's opinion into account when making a decision.[76]

Finally, also relevant is the provision of Art. 876, "Parents exercise parental responsibility in mutual accord."

75 Art. 858 of the Civil Code.
76 Art. 875 of the Civil Code.

The following principles can be deduced from the above regulation. First, parents can make decisions about the child, so they have the right to decide to share a photo, video, quote, etc. Secondly, this right is limited. Parents are limited by the best interests of the child. I confess that I cannot imagine a situation where sharing any information about a child would be in the child's best interest. However, I accept that there may be situations where the impact of such disclosure on a child would be neutral and where it would therefore not be directly contrary to the child's best interests.

Thirdly, there should be a consensus between the parents that photographs or other material relating to the child will be disclosed. And fourth, parents should consider the child's views and not disclose matters without the child's knowledge or against the child's express consent. Here, of course, the problem arises with the maturity of the child, and the ability to evaluate the situation and assess the possible consequences.

Under Czech law, a person acquires legal capacity gradually, in full extent by becoming an adult. Alternatively, in my opinion, Act No. 110/2019 Coll. Act on personal data processing may be considered and applied by analogy. This act provides in Art. 7 that "a child shall enjoy capacity to grant consent to personal data processing in relation to an offer of information society services addressed directly to the child from fifteen years of age." Therefore, I consider the age of 15 years to be a clear threshold in a broader sense, when parents should not disclose anything that may interfere with their child's privacy without the child's consent. In practice, however, parents should also respect the will of the younger child. In fact, the legislation gives the child the opportunity to defend himself against interference with his privacy (and personality) against anyone, including parents exercising parental responsibility.

11. Privacy, digital technologies, and Czech labor law

The issue of the use of digital technologies and privacy protection is also very topical in the field of employment law. The interest of employers in using modern technology to monitor the workplace, and consequently the employee, is understandable. Equally understandable is the desire to monitor an employee's work activities and how he or she uses the resources entrusted to him or her, and whether he or she works during normal work hours. The reasons are many, ranging from protecting the employer's property, ensuring the safety of the employee (typically in hazardous locations such as gas stations), preventing the employee from misusing the employer's property for personal use, but also the interest in the efficiency of the employee's work. Against these interests, which are undoubtedly worthy of protection, stand the interests of the employee and his fundamental rights.

The protection of the employer's property interests and the protection of the employee against unwarranted interference with his or her privacy is ensured by 1) the civil law mechanisms described earlier in this chapter; 2) the regulation in the Labor

Code; and 3) based on the GDPR. For practical reasons, it is the protection through the GDPR that is most often used in employment law practice. It is useful, convenient, and cost-free for employees, as enforcement is delegated to an external state authority.

The legal regulation in the Labor Code generally does not allow employers to interfere in the privacy of employees. However, there is an exception to this general rule. The Regulation is contained in Art. 316 of the Czech Labor Code which states:

> Without a serious cause consisting in the employer's nature of activity, the employer may not encroach upon employees' privacy at workplaces and in the employer's common premises by open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee. (3) Where there is a serious cause on the employer's side consisting in the nature of his activity which justifies the introduction of surveillance (monitoring) under subsection (2), the employer shall directly inform the employees of the scope and methods of its implementation.[77]

The purpose of this amendment is summarized in the explanatory memorandum to the Labor Code. It makes it easier to deal with individual situations, since the previous regulation, which was based on the general constitutional principles arising from the Charter of Fundamental Rights and Freedoms and the application of Art. 7(2) of the previous Labor Code on the principle of good morals, was not satisfactory.[78]

As a rule, employees may not use the means of work entrusted to them by their employer for personal use. This rule also applies to computers, phones, tablets, software, etc., regardless of whether such use is to occur during or after working hours.[79] The employer is therefore allowed to check whether the employee complies with this obligation. However, the tools of control are limited by law.

In particular, the legislation in Art. 316(2) of the Labor Code significantly limits the possibility of control by open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee. According to this provision, on the other hand, it does not matter if an employee is monitored by an online camera that is primarily intended for another purpose and the employer only checks the employee *ad hoc*.[80]

First, under Czech law, the employee must be properly informed that he or she will be monitored by the employer. This information must be provided by the employer to each employee individually and conclusively in his or her own interest. The information should be

77 Art. 316 of Czech Labor Code.
78 See explanatory memorandum.
79 This is, by the way, a common problem in academic practice, as faculty members often use the computer and access to professional databases for private law business or court work.
80 Morávek, 2017, p. 948.

> accurate and complete, and must include a statement of the locations at which the monitoring is carried out, the extent and duration of the monitoring, the technical means by which the monitoring is carried out, whether the data collected, e.g., in electronic form, is retained by the employer, for how long it is retained and for what reason it must be retained.[81]

The obligation to inform is by nature reduced in the case of covert control. However, even in this case, the employer must comply with the information obligation in full immediately, but only after it has been completed; in general terms, the employer must declare the possible control at least in advance.[82]

There must be an *objective and compelling reason* for the monitoring, and it must be carried out in a *proportionate* manner[83] and only in certain places (locker rooms or toilets are strictly excluded, even though these places can be very effectively abused by employees to avoid performing their duties). Monitoring will be excluded whenever the objective of the monitoring can be achieved by other means. Less legally problematic is the situation where the employee is only monitored, and no record would be made. In practice, an employer may incorrectly assess the existence of a reason for interfering with employees' rights. For example, in the case of the State Printing Office (*Státní tiskárna cenin*), which monitored employees extensively, such a reason may indeed exist, but this will be true in the case of printing money, but no longer in a situation where the surveillance was done without the employees' consent and when "only" meal and ticket vouchers were printed.[84]

The possibility of controlling electronic mail is problematic, as there is a risk of violating the confidentiality of letters. Nevertheless, the Art. 316(1) of the Labor Code states that:

> Without their employer's consent, employees may not use the employer's means of production and other means necessary for performance of work, including computers and telecommunication technology for their personal needs. The employer is authorized to check compliance with the prohibition laid down in the first sentence in an appropriate way.[85]

81 Morávek, 2014, p. 953.

82 Ibid.

83 According to the Supreme Court: "The court shall consider, in particular, whether the inspection was continuous or subsequent, its duration, scope, whether it restricted the employee's activities at all and to what extent, whether it also interfered with the employee's right to privacy, etc." 21 Cdo 1771/2011.

84 See case of the Municipal Court in Prague 6 Ca 227/2008 analyzed in Veselý, 2017 Jaké jsou možnosti zaměstnavatele při kontrole zaměstnanců a jak je to s instalací kamer se záznamem? [Online] Available at: https://www.epravo.cz/top/clanky/jake-jsou-moznosti-zamestnavatele-pri-kontrole-zamestnancu-a-jak-je-to-s-instalaci-kamer-se-zaznamem-106015.html?mail (Accessed: 22 June 2022).

85 Art. 316, para. 1 of the Czech Labor Code.

Therefore, an employer may check the inbox and electronic mails, but must do so in a reasonable and proportionate manner. Thus, it is necessary to sensitively assess e-mail after e-mail and evaluate in general whether the individual interference with the employee's rights is necessary. This condition will be fulfilled within the scope of the Czech law if the employee is ill for an extended period, the employment relationship has ended, etc. At the same time, control is possible if the identifying features of the message (sender, subject, address) show that it concerns the employer's activities and is not of a private nature. In general, it is easier to access an e-mail box if the e-mail address is a general e-mail address assigned by the employer to the employee and therefore does not contain the employee's personal identification data.

COVID-19 has greatly expanded the possibilities of working outside the workplace, typically from home. In doing so, the employee is using the resources assigned to the job by the employer and should perform the work at the given time. I believe that in such a situation, the employer cannot exercise control any more than it could in a case where the employee is on-site (*in situ*). The rules described above therefore apply in the same way. I further consider that an employer may order an employee to have a camera on in the case of, for example, work meetings conducted online. However, it cannot prohibit the use of technologies that protect the privacy of the employee and his family, such as blurring the image behind the employee. Finally, I believe that an employer cannot force an employee to agree to record a meeting unless there is a compelling reason to do so.

The possibility of performance of work by electronic means has also led to the fact that the work activities of employees are broadcasted online by electronic means even where it did not happen before, for example in teaching, where teachers must lecture in situ plus accept the fact that their performance is broadcasted online. In addition to that, their work is recorded and published online. I believe that the rules contained in Art. 316 of the Labor Code do not, in principle, prevent the employer from ordering such transmission and recording. It is not related to the employee's control, but to the performance of his or her work, which is public by nature.[86]

Employees often tend to resolve any problems through public law by complaining to the State Labor Inspectorate *(Státní úřad inspekce práce*) or the Office for Personal

86 However, different conclusions can be drawn from the ECtHR's decision in *Antović and Mirković v. Montenegro* (Application no. 70838/13). This is indicated by the fact that the opinion I have referred to is supported by the dissenting opinion of Judges Spano, Bianko and Kjolbro, whereas the decision itself does not contain such reasoning and this concept. Those judges in their dissenting opinion state "We emphasize that the applicants are university teachers who were giving lectures in a university amphitheater, thus fully engaged in a professional activity in a quasi-public setting, and not, for example, in their offices. Having been notified of the video surveillance in the amphitheaters, their reasonable expectation of privacy in that particular context, if any, was very limited. In conclusion, the mere fact of the amphitheaters being monitored cannot in our view engage Art. 8 §1 of the Convention without further elements being demonstrated, as we have explained above. By expanding the scope of Art. 8 §1 to include the facts of the present case, the majority have overly broadened the notion of "private life" under that provision, to an extent which lacks a basis in the Court's case law and is not sufficiently supported by cogent legal arguments."

Data Protection (*Úřad pro ochranu osobních údajů*). Nevertheless, their decisions may be and often are reviewed in court proceedings.

Motivation for employers to violate employees' rights often vary. An example of a situation where an employer has interfered with the rights of employees in an effort to primarily protect his property located in his stores, both from employees and from theft by the public, was a case decided by the Municipal Court in Prague known in the Czech Republic as JRC Czech, a.s.[87] In that case, the court held that

> employees have a right to a certain degree of privacy even in the workplace, even if it is by the nature of the employment relationship, is less than, for example, in the employee's own living quarters, since private life and working life cannot be completely separated; a certain private sphere is constantly worn by the with him and the intrusion into it is, in the case of an employee monitored by CCTV significant in that he is monitored continuously throughout all or most of his working hours every day for the majority of the working day.[88]

The court also stated that the possibility of monitoring of employees in the workplace is not strictly prohibited as the Labor Code allows it under certain circumstances. Nevertheless, according to the court,

> The provisions of the Labor Code must be interpreted in accordance with Section 5(2) of the Data Protection Act, which implies that in addition to a compelling reason based on the special nature of the employer's activities, the interest in protecting the employer's rights or legitimate interests outweighs the interest in protecting the private and personal life of employees.[89]

In this case, however, the conditions for monitoring were not met because the monitoring system was set up inappropriately. The employees were monitored, albeit admittedly (i.e., not covertly), but virtually throughout their working time and at high resolution. As the focus of the system was not on the protection of assets, as declared, but on the monitoring of employees, the employer failed in the test of proportionality.[90]

87 8A 182/2010-69-77.

88 This approach is also supported by the case law of the Constitutional Court, which in turn is based on the case law of the ECtHR, see for example decision of the Constitutional Court Pl. ÚS 3/09.

89 Czech Data Protection Act was replaced by GDPR.

90 The court in this case cited previous decision of the Supreme Administrative Court 5 As 158/2012-4 according to which "installation of CCTV cameras systems, taking into account their nature and the interference with the personal integrity of persons, is only possible when all less invasive means have already failed or would not be able to meet the purpose pursued. There is no doubt that a CCTV system, in comparison with other means (e.g., personnel, mechanical) that can achieve the fulfillment of the purposes pursued by the applicant, interferes with fundamental human rights, namely the right to privacy and to private family life […], and therefore to the human dignity from which those rights derive."

Another case concerned the Czech Post, which massively controlled its employees via GPS locators and as a result 7,770 delivery agents were equipped with trackers.[91] The motivation here was different. The employer defended the tracking for several reasons: 1) to speed up and improve the quality of service and facilitate complaints; 2) to optimize the workload of employees; 3) to monitor the movement and load of vehicles; and 4) to ensure the greatest possible safety of employees at work.

In its decision, the Office for Personal Data Protection did not accept these arguments and stated that this type of monitoring of an employee is unlawful. However, the Office for Personal Data Protection's decision also shows that part of the employer's intention was lawful after all. This was because the aim was also to ensure the benefit of its employees and the persons to whom it provides its services, i.e., to optimize delivery districts in terms of employee workload and complaint handling. The sanction imposed was therefore low — only CZK 80,000.

The decision of the Office for Personal Data Protection has also been reviewed by the courts. The Municipal Court upheld the decision of the Office for Personal Data Protection.[92] In doing so, it considered whether the monitoring of the employees was appropriate, necessary, and proportionate. It found that none of these conditions were met. As regards appropriateness, the technology used could not have prevented the delivery agent from failing to deliver the parcel. The criterion of necessity was also not satisfied since it was sufficient to consider whether the delivery driver approached the delivery point (i.e., the addressee of the parcel). The last criterion, proportionality, was judged not to have been met because of the disproportionate interference with the privacy of the delivery persons (every single movement of the delivery agents was monitored).[93]

On the contrary, the Labor Code does not respond to situations where an employee is recorded, photographed, or monitored by a third party. This could be, for example, a citizen attending a meeting of a public administration body or filming a police officer[94] during an intervention, or a politician in the context of his political activities. A third party can also be a student who films a teacher's online lecture. Undoubtedly, the employer has a duty of prevention in which it should limit the possible risks associated with the performance of the employee's work activity and his right to privacy, if possible. For example, the lecture can be transmitted online under authenticated access and not in full public view, etc.

91 Decision of the Office for Personal Data Protection No. UOOU-00237/13-38.

92 Decision of the Municipal Court in Prague No. 6A 42/2013 5.

93 Bednář and Metelka, 2017, *GPS monitoring zaměstnanců podruhé* [Online] Available at: https://www.epravo.cz/top/clanky/gps-monitoring-zamestnancu-podruhe-106141.html (Accessed: 22 June 2022).

94 Opinion of the Security Policy Department of the Ministry of the Interior on the recording of police officers while on duty.

12. Right to privacy and digital evidence in criminal law

In the field of criminal law, the issue of digital technology and privacy law is particularly relevant in evidence at criminal investigation and trial.[95] According to Art. 89(2) of the Code of Criminal Procedure, evidence can be anything, including audio or visual recordings.[96] The advantage of such evidence is that it is able to provide a range of data and reliably prove a particular fact.[97] It would therefore be a pity not to take advantage of the possibilities offered by modern technology. From a privacy perspective, situations where recordings are made without the knowledge of the person being recorded are problematic. However, it is precisely such recordings that can be of the highest probative value and can also be the only direct evidence. Three key questions have emerged: 1) what procedural conditions must be met for covert surveillance and recording to be possible? 2) Can a privately made recording also be used as evidence? 3) Can evidence obtained by covert recording in one proceeding also be used in another proceeding?

As regards procedural conditions, they are set out in Art. 158d of the Code of Criminal Procedure which regulates the *Surveillance of Persons and Items as follows:*

> (1) Surveillance of persons and items (hereinafter referred to as "surveillance") shall be understood as acquiring knowledge on persons and items conducted in a classified manner by technical or other means. If a Police authority ascertains that the accused person is communicating with his defense counsel, it is obliged to destroy the record containing this communication and not to use facts learned in this connection in any way. (2) Surveillance, during which any audio, visual or other records shall be made, may be performed solely based on written authorization of a public prosecutor. (3) If the surveillance should interfere with the inviolability of residence, inviolability of letters or if it should investigate the contents of other documents and records kept in privacy by use of technical means, it can be performed solely based on prior authorization of a judge. When entering residences, only steps related to the placement of technical devices may be made. (4) Authorization according to sub-sections (2) and (3) may be issued only upon a written request. The request must be reasoned by a suspicion of a specific criminal activity and if known, also by data on persons or items that are to be monitored. The authorization shall state a time limit, for which the surveillance shall be conducted and that cannot exceed six months. The authority that authorized the surveillance may prolong the time limit by a written order issued based on a new written request, always for a time limit not exceeding six months. (5) If the matter cannot be delayed and if cases referred to in sub-section (3) are not

95 The technical aspects of digital evidence are comprehensively described and analyzed in publication Polčák et al., 2015.

96 Art. 89, para. 2 of the Code of Criminal Procedure stipulates: "Evidence may be anything that can help to clarify the case."

97 Deepfake technology relativizes this claim.

> concerned, the surveillance may be initiated even without authorization. However, the Police authority is obliged to immediately request the authorization, and if it is not granted within 48 hours, it is obliged to terminate the surveillance, destroy any eventual records and not use information so ascertained in any way. (6) Without fulfilling the conditions according to sub-sections (2) and (3) may the surveillance be conducted if the person, whose rights and liberties are to be interfered with, grants his explicit consent therewith. If this consent is post facto withdrawn, the surveillance shall be immediately terminated.[98]

From the above it is evident that the Czech legislation distinguishes between 1) surveillance that *does not interfere with the privacy of the monitored person*. In this case, it is the *prosecutor* who gives consent to the surveillance; and 2) situations where *there is an interference with privacy* and therefore a higher level of protection is required. The latter is ensured by the fact that the permission for surveillance must be given by *a judge*. Without the consent of a prosecutor or a judge, the recording is not admissible and thus cannot be used procedurally.

The Code of Criminal Procedure further responds to the issue of modern technology in a relatively new Art. 7b. According to this provision:

> (1) Where it is necessary to prevent the loss, destruction or alteration of data relevant to criminal proceedings which are stored in a computer system or on a medium, the person who holds or has under his control the data may be ordered to preserve such data in an unaltered form for such period as may be specified in the order and to take such steps as may be necessary to prevent disclosure of the fact that the data have been ordered to be preserved. (2) Where necessary to prevent the continuation or repetition of criminal activity, a person who holds or has under his control data stored in a computer system or on a medium may be ordered to prevent other persons from accessing such data. (3) An order under subsection (1) or (2) may be issued by the president of the chamber and, in pre-trial proceedings, by the public prosecutor or police authority. The police authority shall require the prior consent of the public prosecutor to issue such an order; without prior consent, an order may be issued by the police authority only if prior consent cannot be obtained and the matter cannot be delayed. (4) An order under subsection (1) or (2) shall specify the data to which the order relates, the reason for which the data are to be retained or access to them is to be prevented and the period for which the data are to be retained or prevented, which shall not exceed 90 days. The order shall include a statement of the consequences of non-compliance. (5) The authority which has issued an order under subsection (1) or (2) shall promptly deliver it to the person against whom it is directed.

This provision responds to the problem of the ephemeral nature of electronic data. However, there is still no consensus in current practice on how to apply this

98 Art. 158d of the Code of Criminal Procedure.

provision in relation to the provisions of Art. 158d of the Code of Criminal Procedure. A request for data to be "frozen" typically precedes a court's decision that the surveillance may be conducted. Once such a decision is made, however, the police seek the release of the data from the time they receive their request. In practice, this means that the police also request the data that preceded the court's decision. From this perspective, the court's decision could have a retroactive effect, which some attorneys question because of its conflict Art. 158d with the Code of Criminal Procedure.[99]

Interception and recording of telecommunications traffic is carried out based on Art. 88 of the Criminal Procedure Code. In principle, the president of the Senate is authorized to order the interception and recording of telecommunications traffic and, in pre-trial proceedings, judge on the motion of the public prosecutor. They may do so only in specified cases and only in compliance with the principle of proportionality. The possibility of interception and recording of telecommunications traffic in a situation where the accused is communicating with his defense counsel is wholly excluded.

The practical issue is the possibility of using evidence obtained legally in one case to prove another case. Interception and recording of telecommunication traffic carried out based on Art. 88 of the Criminal Procedure Code can, in principle, be used in another case. A recording made during surveillance pursuant to Art. 158d (2) of the Criminal Procedure Code may also be used in another case. For the same conclusion in relation to Art. 158d para. 3, which concerns intrusions into an individual's privacy, a similar permission is missing in the law. This fact limits the possibility of using spatial interceptions as evidence in other criminal proceedings.

13. Private recordings as evidence in criminal and administrative proceedings

The procedural rules allowing surveillance, by which the law restricts the State and its organs, do not naturally apply to individuals — private persons. Nevertheless, the use of a private recording as evidence is not self-evident, as the rights of the person who was recorded must also be respected. The Czech Supreme Court already acknowledged the possibility of using such a recording in 2007 when it stated:

> With regard to the provisions of Art. 89(2) of the Criminal Procedure Code, the possibility of using as evidence a sound recording made by a private person without the consent of the persons whose voice is so recorded cannot in principle be excluded.

99 Odborníkům se nelíbí, že policie žádá o vydání Internetových dat bez souhlasu soudu, 2019, [Online] Available at: https://www.ceska-justice.cz/2019/08/odbornikum-se-nelibi-ze-policie-zada-vydani-Internetovych-dat-bez-souhlasu-soudu/ (Accessed: 07 September 2022).

> Art. 88 of the Code of Criminal Procedure does not apply here, even by analogy. However, the admissibility of such evidence must always be assessed also regarding respect for the right to privacy enshrined in Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and the right to inviolability of the person and his or her privacy within the meaning of Art. 7(1) and Art. 10(2) of the Charter of Fundamental Rights and Freedoms.

In addition, even in the criminal procedure it is relevant whether the facts of the case can also be proved by other/additional evidence.

The Czech courts have addressed the issue of private recording evidence in the following decisions:[100]

Case No. II. ÚS 143/06, in which the Constitutional Court admitted evidence of a covertly made tape recording of a telephone call. It stated:

> The basic criterion which should ultimately lead to a decision on the applicability or inapplicability of the information thus obtained as evidence in the relevant proceedings will be the balancing of the protected rights and interests which clash in this private sphere, and where the state becomes the arbiter (usually through the court) deciding on it, which of these interests will prevail in a given specific conflict, while the assessment of the applicability or inapplicability of the information thus obtained (and submitted to the state in one way or another) will be carried out according to procedural norms, which, however, only define the rules for how to properly determine the facts and find the "substantive" law, i.e., to decide on the actual subject of the dispute. Therefore, in addition to the circumstances in which such a recording was made, the relevance of the interest at stake in the proceedings themselves and the options available to the party claiming that information to obtain that information by means other than at the cost of violating the other person's privacy will be decisive for the final assessment of the case.

Case No. IV. ÚS 2425/09. Here, the Constitutional Court concluded that

> In assessing the objection of violation of the right to privacy by the taking of the said recording, the complainant can be accepted that the monitoring of a public place by a camera and the subsequent taking of a permanent recording fall under the protection provided by Art. 10 of the Charter and Art. 8(8)(a) of the Constitution. In general, to assess whether there has been an unlawful interference with privacy by public authorities, it is necessary to examine whether a private matter or a public event was recorded and whether the material obtained was intended for limited use or was intended to be available to the public…The routine use of security cameras, whether on the street or on premises such as a shopping center or police station, where they

100 The case law of the Czech courts was well mapped in Zaoralová's article (Zaoralová, 2017, pp. 28–32.).

> serve a legitimate and foreseeable purpose, is not in itself problematic in the light of Art. 8 §1 of the Convention…The above conclusions are fully applicable to the complainant's case, since the victim, by installing an industrial camera in a public place, pursued a legitimate aim, i.e., the protection of his property and the detection of the perpetrator of a crime that would affect him personally. The footage was then used only for a strictly necessary purpose (proving the complainant's guilt in criminal proceedings) and was not abused in any way, e.g., by making the footage publicly available, by disparaging the complainant in the media, etc. Therefore, it can be concluded that the installation of the industrial camera and the footage obtained by it does not fulfill the characteristics of a violation of the complainant's constitutionally guaranteed right to protection of privacy.

In contrast to the previous decision concerning monitoring a public place, in the Supreme Court's decision No. 3 Tdo 803/2009, audio and video recordings from a private mobile phone were used as evidence and found admissible.

In a recent decision 3 Tdo 925/2020, the Supreme Court further confirmed and clarified the conditions for the use of a recording made by a private person. The court stated:

> As regards the audio recording made by the victim, nothing prevented its admission as evidence in the case (cf. Supreme Court Resolution of 3 May 2007, Case No. 5 Tdo 459/2007…). Moreover, it was only supporting evidence, while the conclusion of the accused person's guilt was based on the other evidence already mentioned. In the present case, the presence of so-called omitted evidence cannot be found either, since the courts did not omit the defendant's motions for supplementing the evidence, duly dealt with them, and explained why it had rejected them for redundancy.

Another important conclusion follows from the above—in criminal proceedings, evidence that a private person produces himself and that can be used against himself may also be applicable. This may be, for example, a recording from a dashboard camera in a car, from a phone or a smartwatch, i.e., common electronics that we wear and use primarily to help us.

The use of evidence of a recording of a person's image that interferes with that person's personality rights in *administrative proceedings* is based on similar principles to those underlying such use in criminal proceedings. In administrative proceedings, too, there is therefore a distinction depending on who made the recording, whether it was another private person or a public authority. If the recording was made by a public authority, it is applicable only if the law expressly so provides and in addition to that all the conditions required by law must be strictly complied with. In the case of a private person, on the other hand, it may be the case that the statutory conditions are not met (e.g., the qualified consent provided for in the Civil Code is missing or the conditions set out in the GDPR are not fulfilled), but the recording evidence will nevertheless be admissible. According to Supreme Administrative Court, in case

of non-compliance with the law, the administrative court must apply the proportionality test. This test assesses the legitimacy of the objective sought to be achieved by the recording and the proportionality of the procedure used. It is assessed whether, in a particular case, the protection of the personality rights of the subject concerned may outweigh the interest of society in clarifying and punishing the offences and, above all, the protection of the constitutionally guaranteed rights of the maker of the recording.[101]

14. Privacy and COVID-19 — Concluding remarks

Partly outside the substantive framework and focus of the whole chapter is the issue of the measures taken by the Czech Republic during the COVID-19 disease pandemic. The focus of the legislation that applies to this issue lies primarily in the area regulated by the GDPR, which I did not intent to deal with. However, it is a topical issue that relates both to the effective use of modern technology and the protection of privacy. At the same time, the reaction of the Czech State reveals some structural issues that are unfortunately typical of the public administration of the Czech Republic. I will therefore, briefly discuss this issue as well.

In response to COVID-19, the Czech Republic introduced several anti-epidemic measures based on the use of digital technologies. The Tečka and čTečka apps were introduced, and both processed the personal data of individuals. These applications were used to prove and check that a person had been vaccinated or had a valid negative test, or had already had a COVID-19 infection.

But the crux of the problem was that the Czech Republic was unable to adopt a satisfactory and functional legal framework. The Office for Personal Data Protection has criticized this situation. This office has repeatedly called for establishing a clear and permanent framework for the processing of personal data. This office has further criticized that the existing legislation is too general and does not contain any system of graduated legal limits. As a result, the Czech administrative courts repeatedly annulled administrative measures by which the Czech government addressed the problem. At the same time, it would be correct and appropriate for the State to regulate the issue by law instead of administrative measures.

From the point of view of the protection of privacy, it is significant that the Czech sate has made it possible to delegate to private persons the performance of activities carried out in the framework of an epidemiological investigation, which consists of the discovery of information relevant the epidemiological situation. The legal basis

101 2 As 45/2010–68.

for such a transfer is a public contract.[102] The fight against COVID-19 also included tracing the population and the legal regulation of their isolation or quarantine. Notifications of the order for isolation or quarantine were sent orally or in writing by the public health authorities, including by telecommunication. The problem, however, was that the Czech Republic failed to digitize the actual tracing of infected residents. Only the eRouška application was introduced, which theoretically worked on the principle of estimating the probability of infection based on the distance from the contact with the infected person and the duration of the contact. This app could not be described as genuinely functional in practice. The authorities, therefore, routed the contacts of the infected person classically by telephone, and as the pandemic progressed, the system became overwhelmed and essentially stopped working altogether. The state only managed meaningful use of modern digital technologies in relation to crossing state borders as the state used the services of mobile operators to send informational text messages.

It is difficult to assess what was behind the failure of the Czech state to make better use of digital technology to protect public health. Whether it was doubts about how to set up the system so that it did not conflict with the right to privacy, or whether it was a failure to adopt general legislation that would provide the necessary legal basis for the introduction of technical solutions. However, it seems to me that the right to privacy is sometimes used in the Czech Republic as one of those easy and cheap explanations for why some things fail to be implemented by the Czech public administration. COVID-19 and the reactions to it demonstrate this well.

102 Art. 62a of Act No. 258/2000 Coll., the Act on the Protection of Public Health and on Amendments to Certain Related Acts.

Bibliography

Bednář, S., Metelka, J. (2017) *GPS monitoring zaměstnanců podruhé* [Online]. Available at: https://www.epravo.cz/top/clanky/gps-monitoring-zamestnancu-podruhe-106141.html (Accessed: 22 June 2022).

Bónová, K. (2022) 'Ochrana soukromí ve veřejném prostoru', *Revue pro právo a technologie*, 13(25), pp. 157–225 [Online]. Available at: https://doi.org/10.5817/RPT2022-1-4 (Accessed: 22 October 2022).

Dvořák, T. (2014) '§ 135 Ochrana názvu, pověsti a soukromí' in Švestka, J., Dvořák, J., Fiala, J., Pelikánová, I., Pelikán, R., Dvořák, T., Svoboda, K., Pavlík, P. (eds.) *Občanský zákoník – Komentář – Svazek I (obecná část)*. Praha: Wolters Kluwer, pp. 464–471.

Filip, J. (2011) 'Úvodní poznámky k problematice práva na soukromí' in Šimíček, V. (ed.) *Právo na soukromí*. Brno: Masarykova univerzita, Muni PRESS, pp. 9–19.

Nechvátalová, L. (2021) 'Čl. 7 Právo na respektování tělesné a duševní integrity osoby a zákaz mučení a špatného zacházení' in Husseini, F., Bartoň, M., Kokeš, M., Kopa, M. (eds.) *Listina základních práv a svobod. Komentář.* 1st edn. Praha: C. H. Beck. pp. 224–245.

Kočí, P. (2011) *Případ šmírujícího MacBooku – co v Televizních novinách nebylo* [Online]. Available at: https://www.lupa.cz/clanky/pripad-smirujiciho-macbooku-co-v-televiznich-novinach-nebylo/ (Accessed: 22 June 2022).

Kokeš, M. (2012) 'Čl. 12 Soukromí v prostorové dimenzi' in Wagnerová, E. (ed.) *Listina základních práv a svobod: Komentář.* Praha: Wolters Kluwer, pp. 330–340.

Langášek, T. (2012) 'Čl. 7 Nedotknutelnost osoby a zákaz mučení' in Wagnerová, E. (ed.) *Listina základních práv a svobod: Komentář.* Praha: Wolters Kluwer, pp. 186–216.

Lasák, J. (2014) '§ 713 [Ochrana názvu, pověsti a soukromí]' in Lavický, P. (ed.) *Občanský zákoník I Obecná část (§ 1 – 654)*. Praha: C. H. Beck. pp. 711–721.

Míšek, J. (2020) *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita.

Míšek, J. (2017) 'Is the Definition of Personal Data Flawed? Hyperlink as Personal Data (Processing)', in Svantesson, D. J. B., Kloza, D. (eds.) *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*. Cambridge: Intersentia, pp. 331–346; https://doi.org/10.1017/9781780685786.019.

Míšek, J., Kasl, F., Loutocký, P. (2020) 'Czech Republic: Personal Data Protection Law', *European Data Protection Law Review*, 2(6) pp. 289–293 [Online]. Available at: https://doi.org/10.21552/edpl/2020/2/15 (Accessed: 22 October 2022).

Míšek, J., Bartoš, V. (2020) 'Nesnesitelná lehkost zpracování osobních údajů orgány veřejné správy', *Revue pro právo a technologie*, 11(22), pp. 145–174 [Online]. Available at: https://doi.org/10.5817/RPT2020-2-5 (Accessed: 22 October 2022).

Míšek, J. (2014a) 'Consent to personal data processing – The panacea or the dead end?', *Masaryk University Journal of Law and Technology*, 8(1), pp. 69–83.

Míšek, J. (2014b) 'Souhlas se zpracováním osobních údajů za časů Internetu' *Revue pro právo a technologie*', 5(9), pp. 3–74.

Míšek, J. (2014c) 'Vyhledávač jako správce osobních údajů', *Revue pro právo a technologie*, 5(9), pp. 227–229.

Molek, P. (2017) *Základní práva. Svazek první – Důstojnost*. Praha: Wolters Kluwer.

Morávek, J. (2017) '§ 316 Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance' in Pichrt, J. (ed.) *Zákoník práce: Zákon o kolektivním vyjednávání*, Praktický komentář. Praha: Wolters Kluwer, pp. 943–958.

Nonneman, F. (2012) 'Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů', *Právní rozhledy*, 2012/13–14, pp. 505–509.

Ondřejová, E. (2016) *Ochrana osobnosti v common law a českém právu*. Praha: Leges.

Pavlík, P. (2014) '§ 84 Podoba člověka' in Švestka, J., Dvořák, J., Fiala, J., Pelikánová, I., Pelikán, R., Dvořák, T., Svoboda, K., Pavlík, P. (eds.) *Občanský zákoník – Komentář – Svazek I (obecná část)*. Praha: Wolters Kluwer, pp. 321–325.

Pelikán, R., Pelikánová, I. (2014) '§ 3 Zásady soukromého práva' in Švestka, J., Dvořák, J., Fiala, J., Pelikánová, I., Pelikán, R., Dvořák, T., Svoboda, K., Pavlík, P. (eds.) *Občanský zákoník – Komentář – Svazek I (obecná část)*. Praha: Wolters Kluwer, pp. 20–30.

Polčák, R., Púry, F., Harašta, J. (2015) *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita.

Pokorný, M. (2017) *Šmírovaní uživatelé kradeného notebooku si na odškodné počkají. Soud musí případ znovu projednat* [Online]. Available at: https://zpravy.aktualne.cz/domaci/smirovani-uzivatele-kradeneho-notebooku-si-na-odskodne-pocka/r~874defd01f6211e7bc5500259060 4f2e/ (Accessed: 22 June 2022).

Solove, D.J. (2011) *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven: Yale University Press.

Veselý, P. (2017) *Jaké jsou možnosti zaměstnavatele při kontrole zaměstnanců a jak je to s instalací kamer se záznamem?* [Online]. Available at: https://www.epravo.cz/top/clanky/jake-jsou-moznosti-zamestnavatele-pri-kontrole-zamestnancu-a-jak-je-to-s-instalaci-kamer-se-zaznamem-106015.html?mail (Accessed: 22 June 2022).

Wagnerová, E. (2012) 'Čl. 10 Právo na soukromí v širším smyslu' in Pospíšil, I., Langášek, T., Šimíček, V., Wagnerová, E. (eds.) *Listina základních práv a svobod: Komentář*. Praha: Wolters Kluwer, pp. 277–299.

Zaoralová, P. (2017) 'Použitelnost soukromých zvukových a obrazových záznamů jako důkazu v trestním řízení', *Bulletin Advokacie*, 2017/11, pp. 29–34.