Chapter 14
Right to Privacy: A (re-)measurement

Doris Hattenberger and Florian Vidreis

Abstract Essays on the right to privacy now include by default the observation that privacy is more at risk than ever. This is due to technological progress, which has made the threat decentralized and ubiquitous, and assaults are cheap for everyone. In addition, many are highly permissive with data from their private lives. Has privacy protection, therefore, become obsolete? Not at all. Apart from a core area of privacy that is considered to be unalterably protected, it must be constantly redefined in view of the dynamics of developments. This article attempts to make the contours of privacy protected by fundamental rights visible.

14.1 Introduction

"Privacy is doomed . . . get used to it." With this headline, more than 20 years ago, *The Economist* accurately described a development that some call the post-privacy age (Berka, 2018, p. 756). There is no shortage of scandals to substantiate this development: in the "Cambridge Analytica" case, the company unlawfully analyzed up to 87 million Facebook users' profiles. Cambridge Analytica created profiles from the data obtained to use them in the US election campaign and the Brexit vote (see Mueller et al. in this volume). In 2013, Edward Snowden informed the public that the US intelligence agency NSA monitored global Internet communications without restraint. Besides, the British government systematically monitored politicians from other nations by spying on their emails and computers during the G20 summit. We have become familiar with data theft reports or unauthorized data disclosure, especially to other companies.

Florian Vidreis prepared the case law examples, and Doris Hattenberger wrote the remaining text.

D. Hattenberger (✉) · F. Vidreis
Alpen-Adria Universität Klagenfurt, Klagenfurt, Austria
e-mail: doris.hattenberger@aau.at; Florian.Vidreis@gmx.at

M. Karmasin et al. (eds.), *Media and Change Management*,
https://doi.org/10.1007/978-3-030-86680-8_14

However, the loss of privacy is by no means solely the result of frequent breaches of the law. It is generally the rapidly changing technical possibilities that dissolve familiar boundaries between public and private. Anyone who wants to use the smartphone's advantages, which is today a "mainframe," inevitably leaves many traces on the Internet. With the possibilities of big data and data mining, personality profiles can be generated to predict people's behavior better than their closest relatives and best friends can (see Malthouse and Green in this volume). Cross-border networking and the associated globalization of data flows mean that the national legislators' control options can only have a limited effect. The question of responsibility is becoming increasingly difficult to resolve (see Voci and Karmasin in this volume). The narrowing space of the private sphere is due not least to the decentralization of the threat. Whereas protection from an overpowering state used to be the primary concern, today, the danger also comes primarily from private individuals. There are many of them, considering that more than 4 billion people use the Internet today (Berka, 2018, p. 756).

The decentralization of the threat to privacy is a direct consequence of product convergence (Diehl & Karmasin, 2013, p. 1; Diehl et al., 2013, p. 353f; Terlutter & Moick, 2013, p. 164f). A smartphone is no longer just a phone but a multifunctional device. It is suitable for individual as well as mass communication. Whereas in the past, the operation of a mass medium such as a newspaper or a radio station was reserved for only a few because of the high investment costs, mass communication possibilities are now open to everyone. Also, today's smallest devices, which one can buy cheaply in shops, offer control possibilities that were previously only available to state security agencies. Product convergence makes it possible for many people to invade the privacy of others.

Invasion of privacy is cheap and easy to have today. The computer as a work tool and companion gives the employer extensive control possibilities. For example, they can obtain information on when, with whom, and how long communication took place or which documents were written or printed, and how quickly. In the digital age, these control options are technical by-products, data that accumulates, but at the same time they can reach far into the private sphere.

The state's surveillance instruments significantly expanded in recent years. Austria introduced the "Great Wiretapping Attack" and the "dragnet" as far back as the end of the twentieth century (Berka, 2012, p. 10, 2020, p. 498). It was followed by preventive video surveillance, for example, at crime hotspots or—in the wake of the Madrid and London attacks—the adoption of the Data Retention Directive by the European Union (see Mueller et al. in this volume). This Directive required telecommunications service providers to store traffic and location data (but not content data) in the telecommunications sector for a legally standardized period to prevent, detect, investigate, and prosecute serious crimes and protect state security.

On the one hand, the private sphere's erosion is caused by the technical possibilities to penetrate it. On the other hand, users of the blessings of technology are more willing to disclose personal information. Not only fitness data such as weight, pulse rate, and oxygen saturation are shared but also what one is currently reading, streaming, or eating (Berka, 2018, p. 756). In addition, the possibilities of the new

communication and information technologies not only create new threats but are also accompanied by conveniences and advantages. They offer new opportunities for social interaction and an increase in comfort. "In this sense, the growth and loss of freedom go hand in hand" (Berka, 2012, p. 11). Apart from that, not using these technologies today means being an outsider and being isolated in social and economic terms. It is almost impossible to get out.

This situation raises the question of what we are talking about when we speak of a right to privacy. It may well be that, as a result of these developments, the protected area is becoming increasingly smaller and that some people are also voluntarily giving up this protection to a large extent. However, this does not change the necessity of protecting privacy. On the contrary, the almost overwhelming threat potential has only strengthened the insight into safeguarding the private sphere. Privacy is an essential prerequisite for the development and unfolding of the personality. It is a space of retreat, an area in which one feels safe. People who think they are constantly being watched come under pressure to conform and behave differently than they would without control (Wiederin, 2014, p. 364). And the Austrian Constitutional Court (VfGH) has very aptly described the need to protect privacy as follows: "In a society characterized by respect for freedom, the citizen need not, without good reason, allow anyone to see what pastime he pursues, what books he buys, what newspapers he subscribes to, what he eats and drinks, and where he spends the night" (VfGH 14.03.1991, G 148/90, ECLI:AT:VFGH:1991:G148.1990).

In the following, the private sphere's legal guarantees, its status in the legal system, will be presented. However, the starting point is the Austrian legal system, which is intensively influenced by European law. In this respect, we are also talking about a European body of law. Examples from case law will measure the scope of protection of the right to privacy. It will be shown that this is not a fixed value but is changeable and, above all, disposable. It is up to the individual to determine what they want to reveal to others and what they want to keep secret.

14.2 Fundamental Right to Privacy

14.2.1 Right to Privacy in the Multilevel System of the Legal Order

The Austrian legal system robustly and repeatedly protects the right to privacy. One should note that this right is guaranteed at several levels of the legal system. First, the Austrian legal order is hierarchical—a system of norms in a relationship of superiority and subordination. Excluding the European Union law, constitutional law is at the top of this hierarchy. The following are the simple laws, regulations, and individual decisions such as notices and judgments. These norms are in a relationship of superiority and subordination because the superior law regulates the formal

and substantive conditions for the generation of subordinate law. An example will show this. Suppose the Austrian constitutional order provides for a so-called fundamental right to privacy. In that case, the legislator who enacts simple laws is bound by the value decisions expressed by this fundamental right when enacting the simple laws. On the other hand, this means that a simple-law provision that does not duly respect the fundamental right to privacy provided for in the Constitution is unconstitutional and will be overturned in proceedings before the Constitutional Court. Accordingly, norms with a higher rank determine subordinate law. Provisions for the protection of privacy can be found at several levels, both at the level of constitutional law and at the level of simple statutory law.

The European Convention on Human Rights (ECHR) is a treaty under international law that was drawn up within the framework of the Council of Europe, signed in 1950, and entered into force in 1953. Austria acceded to the Convention in 1956 and adopted it directly into domestic constitutional law. It, therefore, has the status of national constitutional law. The significance of the Convention for the development of human rights protection is outstanding. It is a highly developed catalog of human rights (at the time). Furthermore, it provides a legal protection system that allows individual persons (and not only states) to sue for violations of the guaranteed human rights before an international authority, the European Court of Human Rights (ECtHR). In turn, this Court's decisions influence the interpretation and application of the Convention rights by national authorities.

The right to privacy is also guaranteed in other international legal documents that strongly impact the Austrian legal system. One of these is the Charter of Fundamental Rights of the European Union (CFR), which protects several aspects of privacy in Article 7 and Article 8. Due to the specific mode of action of Union law, these guarantees have the quality of rights guaranteed by constitutional law. Accordingly, they have the same status as nationally assured fundamental rights (Riesz, 2019, margin 26).

Last but not least, the Council of Europe Convention 108 of 28 January 1981 for the Protection of Individuals concerning Automatic Processing of Personal Data should be mentioned in this context. This Convention was the first internationally binding document that protects individuals against attacks through the use of personal data. This international Convention is still in force today (Forgó & Rieß, 2018, margin 16).

14.2.2 How Fundamental Rights Work

Fundamental rights are "fundamental legal positions" of human beings, legal positions that society regards as essential and indispensable, intended to protect the individual's dignity and freedom (Berka, 2020, p. 403). They enjoy a higher status than other legal claims: They are warranted in constitutional law and thus also endowed with a higher substantive power because they can only be amended in

parliament by a majority of two-thirds of the votes cast. They are, therefore, beyond the control of a simple majority in parliament.

An essential feature of fundamental rights is that individuals can enforce them.

Following their historical significance, fundamental rights are directed against the state. They regulate the relationship of the state to its citizens.

The first catalogs of fundamental rights emerged in Austria in the middle of the nineteenth century. The enlightened middle classes demanded that the state respect a sphere of freedom. Accordingly, fundamental rights were to protect the individual from interventions by the state upon this sphere of freedom. They were conceived as so-called defensive rights. The state was required to refrain from interfering with this sphere of freedom.

However, the effect of fundamental rights has long since been tied to more than just the state's failure to act. In addition to the defensive dimension of fundamental rights, they also give rise to duties on the state's part to protect. It means that the state must take (active) action. The freedom rights also oblige the state to protect from interference by third parties. For example, Article 8 of the ECHR, which requires respect for private life, implies that the state must also actively protect individuals from emissions that are harmful to their health (ECtHR 28.01.2000, 21,825/93 and 23,414/94, *McGinley and Egan* vs. *The United Kingdom,* ECLI:CE:ECHR:2000:0128JUD002182593). Furthermore, it is also derived from Article 8 ECHR that the state must establish effective legal protection to enable individuals to enforce their rights (Meyer-Ladewig & Nettesheim, 2017, margin 2f). Finally, Article 8 ECHR also obliges the state to enact penal laws to effectively prevent severe violations of the values protected by Article 8 ECHR. The European Court of Human Rights considered Article 8 to be violated because the punishment of rape requires proof of physical resistance (ECtHR 04.12.2003, 39,272/98, *M.C.* vs. *Bulgaria,* ECLI:CE:ECHR:2003:1204JUD003927298).

14.2.3 Test Scheme: Intervention and Violation

Human rights documents do not guarantee fundamental rights in absolute terms. States can restrict the guarantees of liberty to protect higher-value public interests or to protect others' freedoms. It is essential to distinguish between intervention and infringement. In a first step, one has to examine whether the measure intervenes in the protected sphere of the fundamental right. In a second step, one has to find out whether the intervention is justified or inadmissible. In the latter case, one speaks of a violation or infringement of the fundamental right (Berka, 2020, p. 445). Such an infringement is assumed if an intervention on the fundamental right is not provided for or if the intervention's constitutional conditions are not met. For example, the fundamental right is violated if there is no legal basis for the intervention, or because no legitimate objective of the intervention is being pursued, or because the encroachment is disproportionate. The requirement of proportionality then includes further test steps:

1. The means used must be suitable to achieve the goal.
2. The means used must be necessary, i.e., always use the mildest means to achieve the objective.
3. An appropriate relationship must be maintained between the severity of the intervention on fundamental rights and the weight of the legitimate objective pursued. Therefore, a grave intervention on a fundamental right violates the fundamental right if the interest pursued is of minor importance.

14.2.4 Legal Protection

Fundamental rights are subjective rights. That means that they can also be enforced by those affected. As they are guaranteed at various legal system levels, they also provide legal protection before various national and international authorities.

At the national level, the Austrian Constitutional Court (Verfassungsgerichtshof, VfGH) is primarily responsible for safeguarding fundamental rights. On the one hand, it examines general legal acts (e.g., laws) to determine whether they are compatible with fundamental rights. However, it also investigates possible violations of fundamental rights by individual decisions of the administrative courts. The Supreme Court (Oberster Gerichtshof, OGH), Austria's highest court in civil and criminal matters, is also responsible for ruling on violations of fundamental rights.

If the ECHR's rights are violated, an international court, namely, the European Court of Human Rights (ECtHR), can be called upon after the domestic possibilities have been exhausted.

The European Court of Justice of the European Union (ECJ) decides on violations of rights under the Charter of Fundamental Rights.

The decisions of the two international courts, also in non-Austrian cases, are of particular importance for national legal practice, especially since they provide important indications for the interpretation of fundamental rights even by the state authorities. In this respect, one can justifiably speak of a European standard of fundamental rights.

14.2.5 The Fundamental Right to Privacy

Genuinely national constitutional law protects individual aspects of privacy. In particular, these are the inviolability of the right of domicile (Article 9 Basic Law on the General Rights of Nationals, StGG), the secrecy of correspondence (Article 10 StGG), the secrecy of telecommunications (Article 10a StGG), and the fundamental right to data protection (§ 1 Data Protection Act, DSG). Article 8 ECHR, on the other hand, protects private and family life in general; also, it protects the home and correspondence. Article 7 CFR protects private and family life, home, and communication. Article 8 CFR guarantees the right to protection of personal data.

Together, these provisions comprehensively protect privacy; the scope of application overlaps in part, but the conditions for interference are different. Article 8 ECHR and Article 7 CFR's safeguarding of private and family life has a particular catchall function. The broad notion of private and family life is open enough to accommodate novel threats posed by new technologies (Wiederin, 2002, margin 4). Altogether, they protect human privacy (Wiederin, 2002, margin 6; Grabenwarter & Pabel, 2021, p. 294).

From a historical perspective, partial aspects of privacy—namely, the protection of the right of the home and respect for the secrecy of correspondence—are among the oldest fundamental rights in the Austrian catalog of fundamental rights. Both rights were already enshrined in continental Europe in the mid-nineteenth century. The comprehensive protection of private and family life has been guaranteed since the middle of the twentieth century, on the one hand, by the Universal Declaration of Human Rights 1948 (Article 12) and then by Article 8 ECHR (Wiederin, 2002, margin 1).

14.3 Right to Respect for Private Life

14.3.1 Protected Scope

According to Article 8 ECHR, everyone is entitled to "respect for his private and family life, his home and his correspondence." The scope of protection of this fundamental right is the individual's personality in its uniqueness, which also manifests itself in the encounter and exchange with others. However, the self-determined lifestyle, the right to live a life according to one's ideas, is protected (Berka 2020, p. 487; Berka et al., 2020, p. 356; Öhlinger & Eberhard, 2019, margin 812; Wiederin, 2014, p. 374; Bezemek, 2016, p. 148; Meyer-Ladewig & Nettesheim, 2017, margin 7; Grabenwarter & Pabel, 2021, p. 296, margin 6).

The delimitation of the scope of protection is difficult and also changeable. The content is strongly influenced by social conventions and moral concepts and must therefore be reassessed continuously (Wiederin, 2002, margin 7). However, indisputably the intimate and secret spheres are within the scope of application. Furthermore, behavior that appears in public, such as a visit to the theater or a stay in the hospital, or even renting a movie in a public video store, is protected (VfGH 14.03.1991, G 148/90, European Case Law Identifier ECLI:AT:VFGH:1991:G148.1990). The need for protection is also different. It is high when it concerns the most intimate area of the person. This area includes sexual life, health, illnesses, or relationships with partners, family members, friends, or confidants. And a high need for protection also exists when people think they are unobserved (Berka et al., 2020, p. 358). It is lower if the behavior takes place in public or one even addresses it to the public (Grabenwarter & Pabel, 2021, p. 299). To put it in a few examples: Disposing of one's own body, even after death, is part of a person's protected private life (VfGH 08.10.2014, G 97/2013; ECLI:AT:VFGH:2014:G97.2013); the same

applies to telephone calls, email, and Internet use at the workplace (ECtHR 03.04.2007, 62,617/00, *Copland* vs. *the United Kingdom,* ECLI:CE:ECHR:2007:0403JUD006261700) or the private use of messenger services intended for business use, even if the employer has prohibited private use (ECtHR 05.09.2017, 61,496/08, *Barbulescu* vs. *Romania* (Grand Chamber), ECLI:CE:ECHR:2017:0905JUD006149608). The right to private life can also be violated if the state refuses to change a person's name after a gender reassignment or does not permit a marriage. Interventions on the right to private life also occur when third parties gain access to information from the private sphere, such as secret surveillance measures, telephone tapping, the unwanted publication of photos, or surveillance by a camera in public places (Öhlinger & Eberhard, 2019, margin 814). The technical possibilities which are available to everyone today favor such information interventions.

Article 8 ECHR also guarantees a right of access to one's health data after hospitalization (ECtHR 28.04.2009, 32,881/04, *K.H.* et al. vs. *Slovakia,* ECLI:CE:ECHR:2009:0428JUD003288104) or to environmental information if it presents a risk to data subjects. It also protects the formation of identity. The right to receive information about the essential aspects of one's identity is also covered by the protection of private life (Meyer-Ladewig & Nettesheim, 2017, margin 22).

In its defensive dimension, the fundamental right is directed against the state. The state must refrain from intervention unless it is justified. Apart from this, the state is also obliged to protect the right to respect for private life from encroachment by third parties. For example, the state has to prevent interventions on personal integrity by third parties through appropriate penalization. The lawmakers also have to protect the honor of the individual through proper regulations, to sanction rape under criminal law (ECtHR 26.03.1985, 8978/80, *X and Y* vs. *The Netherlands,* ECLI:CE:ECHR:1985:0326JUD000897880), and to take adequate precautions to ensure that personal data such as an HIV infection are not disclosed (ECtHR 25.02.1997, 22,009/93, *Z* vs. *Finland,* ECLI:CE:ECHR:1997:0225JUD002200993). The legal system must also protect the individual from unnecessary disturbance by prohibiting anonymous telephone calls or the installation of surveillance cameras. Protection against assault must also be provided in private employment relationships. If the employer pronounces a dismissal because of an extramarital relationship of an organist (ECtHR 23.09.2010, 1620/03, *Schüth* vs. *Germany,* ECLI:CE:ECHR:2010:0923JUD000162003) or because of specific clothing such as the wearing of a pink hairband by a bus driver (OGH 24.09.2015, 9 ObA 82/15x, ECLI:AT:OGH0002:2015:RS0130288), this contradicts Article 8 ECHR (Berka, 2018, p. 488; Berka et al., 2020, p. 361; Bezemek, 2016, p. 158).

The fundamental right to protection of private life is not protected in absolute terms. Once an interference has been established, the second step is to examine whether the interference is permissible. If the admissibility check fails, then there is a violation. Interference is permitted under the following conditions: It must be

– Provided for by law
– And must be necessary in a democratic society to achieve specific objectives set out in Article 8 (2)

Accordingly, interference is only permissible if a law authorizes it. The more intensive the interference with the fundamental right, the more precisely the legal authorization for the interference must be described. For example, secret wiretapping measures are a particularly intensive intervention in the fundamental right to private life. The prerequisites for such measures must be specified in detail in the law (Meyer-Ladewig & Nettesheim, 2017, margin 37; Wiederin, 2002, margin 19).

Article 8 (2) ECHR lists national security, public peace and order, the economic well-being of the country, the defense of law and order, the prevention of criminal acts, the protection of health and morals, and the protection of the rights and freedoms of others as legitimate objectives. National security plays a role in connection with telephone surveillance, for example. Restrictions in connection with detention may be justified by public peace and order. The justification of protecting the rights and freedoms of others includes, for example, the protection of minors or the protection of secrets (Wiederin, 2002, margin 23). The legislature may regulate people's sexual lives only to the extent that it affects others' rights or public order. If prostitution, however, does not appear outwardly, then a ban is not necessary in a democratic society and is therefore inadmissible (VfGH 09.03.1978, G 63/77; ECLI:AT:VFGH:1978:G63.1978). A compulsory blood sample is only permissible as an intervention on bodily integrity if a weighty interest justifies it. The scope of protection of private life also includes the identity of a person. The denial of a name change after a gender reassignment (ECtHR 25.03.1992, 13,343/87, *B* vs. *France,* ECLI:CE:ECHR:1992:0325JUD001334387) is a violation of Article 8 ECHR. Also covered by the scope of protection is the right to indicate a third or no gender in civil status records (VfGH 15.06.2018, G 77/2018, ECLI:AT:VFGH:2018:G77.2018).

Article 8 ECHR also applies to information interventions that are only permissible if a law authorizes them and they are justified by public interest and withstand a proportionality test. In recent years and decades, state authorities have been granted extensive surveillance powers, such as large-scale eavesdropping, dragnet searches, cell phone tracking, and access to private computers, which allow deep penetration into the private sphere. These instruments are particularly intrusive because they are used without the knowledge of those being eavesdropped on or observed in an area where the persons concerned believe they are unobserved. Such interventions are only justified if there are particularly weighty reasons—such as organized crime or terrorist attacks—and mechanisms are provided to protect against abuse. Surveillance powers, which are typical for a police state, can only be permissible in a democratic society in exceptional situations and within narrow limits (ECtHR 06.09.1978, 5029/71, *Klass* vs. *Germany,* ECLI:CE:ECHR:1978:0906JUD000502971*;* Berka, 2020, p. 490).

14.3.2 Examples of Case Law

The installation of a covert video surveillance system used by an employer to film cashiers at a Spanish supermarket was the subject of a case before the ECtHR. Cashiers claimed a violation of Article 8 ECHR because the surveillance system had been installed without their knowledge. The employer had had the system installed on suspicion of theft. This suspicion was also confirmed by analysis of the video material. The Third Chamber (ECtHR 09.01.2018, 1874/13 and 8567/13, *López Ribalda* et al. vs. *Spain* (Third Chamber), ECLI:CE:ECHR:2018:0109JUD000187413) qualified the measure as disproportionate because it meant a significant invasion of the privacy of the persons concerned.

Furthermore, the employer could have informed the female employees as a palliative measure. The Grand Chamber of the ECtHR disagreed. Due to the short duration of the secret surveillance and the limited possibilities available to the employer to protect its property, it was not considered a violation of Article 8 ECHR (ECtHR 17.10.2019, 1874/13 and 8567/13, *López Ribalda* et al. vs. *Spain* (Grand Chamber), ECLI:CE:ECHR:2019:1017JUD000187413).

In the *Barbulescu* case (ECtHR 12.01.2016, 61,496/08, *Barbulescu* vs. *Romania* (Fourth Chamber), ECLI:CE:ECHR:2016:0112JUD006149608), the employee was requested by his employer to create an account on the Yahoo messenger service to respond to customer inquiries. According to the employer's instructions, the employee was only allowed to use the account for professional purposes. Subsequently, the employee used it for private purposes as well. The employer recorded the use in real time, and Barbulescu was dismissed because of the personal use. The Grand Chamber of the ECtHR considered this measure to be a violation of Article 8 ECHR. The employer should have informed the employee before the start of the monitoring and explained the monitoring details. Immediate control of the content of the communication without a reminder contradicts the principle of transparency (ECtHR 05.09.2017, 61,496/08, *Barbulescu* vs. *Romania* (Grand Chamber), ECLI:CE:ECHR:2017:0905JUD006149608).

The publication of photographs is an interference with private life protected by Article 8 ECHR. In *Caroline von Hannover v. Germany* (ECtHR 24.06.2004, 59,320/00, *Von Hannover* vs. *Germany*, ECLI:CE:ECHR:2004:0624JUD005932000), the court made fundamental statements. In the context of balancing the right to freedom of expression and the protection of privacy, the court held that what mattered was whether the publication of the photographs contributed to a public debate of general interest. This argument also applies to public figures.

14.4 Protection of the Home

The inviolability of the right of the home is one of the oldest fundamental freedoms of the national constitutional order. Protection against arbitrary house searches was already granted by the law of 27.10.1862 on home law protection. It is now guaranteed in Article 9 StGG. Besides, Article 8 ECHR and Article 7 CFR guarantee a right to respect for the home. This right also serves to protect privacy. It intends to ensure a space of retreat for the individual, protected from intrusion by third parties. In addition to dwellings, the scope of protection also includes outbuildings, rooms used for business purposes, houseboats or mobile homes. The term "dwelling" is to be interpreted broadly (Öhlinger & Eberhard, 2019, margin 396; Meyer-Ladewig & Nettesheim, 2017, margin 89; Grabenwarter & Pabel, 2021, p. 336).

The right of domicile, according to Article 9 StGG, offers protection against unjustified house searches; this means the intrusion into the "dwelling or other premises belonging to the household" for the purpose of searching for persons or objects. A house search is only permissible if a law authorizes it and, in principle, the individual house search was authorized by a judge. The necessity of a judicial order is an expression that the home is exceptionally protected.

The protection afforded by Article 8 ECHR goes further. It protects against unjustified house searches and intrusion into the home without the consent of the owner. This also includes, for example, the unauthorized installation of listening devices and video cameras (Berka, 2020, p. 502).

14.5 Protection of the Communication

Communication is constitutionally protected in different ways and with different requirements. According to Article 10 StGG, the secrecy of correspondence is inviolable. Sealed documents that are not intended for outsiders are covered by the scope of protection. Interference occurs when sealed documents are opened to gain knowledge of their contents. An intrusion is permissible if it takes place in the context of a legal arrest or house search, in cases of war, and if a judge has approved the opening in advance (Berka, 2020, p. 503; Öhlinger & Eberhard, 2019, margin 381).

Again, the protection of correspondence by Article 8 ECHR goes further. It protects not only written communication but also telephone conversations. Interference is also present if the correspondence is hindered by state authorities, for example, if prisoners' mail is not forwarded. According to the well-known formula of Article 8 (2), interference is only permissible if a legitimate aim is pursued and the measure is suitable, necessary, and proportionate. The Constitutional Court considered monitoring a prisoner's correspondence with his lawyer to be unconstitutional because postal communication with the lawyer must be possible on a confidential basis (Berka, 2020, p. 504).

The right to respect for the correspondence requires the state not only to refrain from intervening but also to act actively. For example, Article 8 ECHR is also violated if prisoners are not provided with sufficient writing material to communicate with the court (ECtHR 24.02.2009, 63,258/00, *Gagiu* vs. *Romania,* ECLI:CE:ECHR:2009:0224JUD006325800).

Article 10a StGG protects the secrecy of telecommunications. It covers the communication transmitted via telecommunications networks, thus the telephony, email correspondence, and other information sent via radio or communications networks. Article 10a StGG protects the content of communications; external communications data such as names, telephone numbers, locations, call durations, or IP addresses are not covered. According to Article 10a StGG, monitoring the content of communications requires prior judicial approval. The judge's reservation further proves that the constitutional legislator intended that the protected freedom needs special protection. For external communications data—also known as traffic data—Article 8 ECHR provides protection (Berka, 2020, p. 504; Öhlinger & Eberhard, 2019, margin 826).

In recent years, the powers of the security police to conduct surveillance have been considerably expanded. These include, for example, the collection of call data with the obligation of providers to transmit IP addresses or the tracking of the location to prevent threats to the life or health of people.

14.6 Protection of Personal Data

14.6.1 Scope of Application

Section 1 of the Austrian Data Protection Act (DSG) guarantees a fundamental right to data protection. This fundamental right intends to set limits on the virtually unlimited technical possibilities for processing personal data. First of all, it guarantees personal data confidentiality, provided that there is a legitimate interest in such secrecy. "Personal data" is defined as all information relating to a person. The name is just as much personal data as physical characteristics, value judgments, IP addresses, biometric characteristics, illnesses, party affiliation, etc. It is only essential that one can assign this information to a specific person. If personal data is generally available or data cannot be traced back to a particular person, there is no interest in confidentiality worthy of protection. Because of their general availability, data that can be viewed in public books (such as the land register) are therefore not protected by Sect. 1 of the Data Protection Act. The fundamental right to data protection protects against collecting and disclosing personal data (Jahnel, 2020, p. 537; Eberhard, 2016, margin 45; Pollirer et al., 2019, margin 1).

The personal scope of the fundamental right to data protection covers both natural and legal persons. This means that companies can also invoke this fundamental right to protect their economic data. This circumstance is remarkable in that the General Data Protection Regulation only covers the data of natural persons (Jahnel, 2020,

p. 537; Pollirer et al., 2019, margin 3). When a person dies, the protection afforded by the fundamental right ends. This is justified with the argument that the right to data protection has a highly personal character. However, the honor and privacy of a deceased person—especially the "image of life"—are not without protection. Post-mortem protection guarantees Article 8 ECHR (Eberhard, 2016, margin 27).

The fundamental right to data protection has gained enormous importance in the recent past. This increase in importance is in step with the rapidly expanding possibilities of technological progress in information and communication technologies. Almost unlimited networking, storage, and evaluation possibilities allow deep penetration into the individual's privacy (Eberhard, 2016, margin 2). The protection goal is to enable and secure confidential communication between people (VfGH 27.06.2014, G 47/2012 et al., ECLI:AT:VFGH:2014:G47.2012).

The fundamental right to data protection is also not protected in absolute terms. For example, a violation of the fundamental right does not occur if the processing is carried out in the data subject's vital interest. This would be the case, for example, if a person's life is in danger and he or she urgently needs help but is no longer able to consent to data processing due to his or her condition. Furthermore, personal data processing is also permissible if the person concerned has given his or her consent. This is referred to as the right to informational self-determination and means that it should be up to the individual to decide how much of their private life they wish to share with others. Finally, the fundamental right to data protection can be restricted if a statutory provision authorizes this, if this provision pursues a legitimate interest, and if the principle of proportionality is observed. For example, a radio cell analysis to investigate an offense punishable by more than 1 year's imprisonment is only proportionate if this measure is limited to a short period. The secrecy of communications of completely uninvolved persons may only be interfered with to the extent that this is unavoidable (OGH 05.03.2015, 12 Os 93/14i, ECLI:AT:OGH0002:2015:RS0129979).

Under Sect. 1 of the Data Protection Act, the right to secrecy is supplemented by accompanying fundamental rights, which are also guaranteed by constitutional law. These include the right to information, the right to rectify inaccurate personal data, and the right to erase inadmissibly obtained personal data (Sect. 1 (3) of the Data Protection Act).

The mass collection of personal data in the context of so-called section control requires precise regulations on data collection and data use that make such interventions foreseeable (see Mueller et al. in this volume). Statistical surveys that include personal data are an encroachment on fundamental rights. However, they can be justified if the country's economic well-being requires them, if they are limited to the necessary extent, and if precautions are taken to ensure confidentiality (VfGH 15.06.2007, G 147/06 et al., ECLI:AT:VFGH:2007:G147.2006).

At the EU level, Article 7 CFR guarantees every person a right to protection of personal data concerning them.

14.6.2 Examples of Case Law

In the wake of 9/11 and the attacks in Madrid and London, the EU issued the so-called Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 2006/105, 54). This Directive requires that so-called traffic data generated in the course of telephony, email, and Internet communications, such as master data, location data, IP address, (Internet) telephone service provider, and time of connection establishment, but not content data, be stored for at least 6 months and a maximum of 2 years without any reason. The Directive aimed to combat serious crime. The ECJ examined this Directive for its compatibility with Article 7 and 8 CFR. The ECJ found a violation of Article 7 and Article 8 CFR because the Directive generally applies to all persons and all electronic means of communication and all traffic data without any differentiation, limitation, or exception (ECJ 08.04.2014, C-293/12 and C-594/12, *Digital Rights Ireland,* ECLI:EU:C:2014:238). Accordingly, it also applies to persons who have no connection with a serious crime or whose communications are subject to professional secrecy under national regulations. The Directive also does not provide any objective criterion concerning the restriction of access, the number of persons authorized to access the data, and the storage period's determination. In this respect, the required limitation to what is absolutely necessary is missing, and also, the requirement of precise prior determination of the intervention on fundamental rights is not met.

The decision of *Google Spain* and *Google* (ECJ 13.05.2014, C-131/12, *Google Spain SL, Google Inc.,* ECLI:EU:C:2014:317) attracted particular attention. The proceedings' subject was the request of a Spaniard to delete a specific result of a search for a newspaper report. When entering his name in the Google search engine, users were shown links to a third party's newspaper reports. In these newspaper reports, his name was mentioned in connection with the sale of a property due to a seizure. The person concerned demanded deletion from the newspaper company as well as from Google Spain and Google Inc. He was successful against the search engine operator Google. First, the court affirmed the applicability of Article 7 CFR because Google also operates a branch in Spain. Accordingly, EU law was applicable. The ECJ also confirmed a right to deletion or to be forgotten against the search engine operator, regardless of whether the information still appears elsewhere on the Internet. The deletion of the search results complies with the fundamental right to data protection (ECJ 13.05.2014, C-131/12, *Google Spain SL, Google Inc.,* para 19, ECLI:EU:C:2014:317). This decision is one of the most significant in the recent past. According to another decision of the ECJ, the delisting must be carried out for all Member States, but not for all country versions (ECJ 24.09.2019, C-507/17, *Google LLC* vs. *Commission nationale de l'informatique et des libertés (CNIL),* para 73, ECLI:EU:C:2019:772).

In two equally important decisions, the ECJ found that the level of data protection guaranteed in the USA by the Safe Harbor and Privacy Shield agreements does not meet the requirements of Article 7 and 8 CFR (*Schrems I*, ECJ 06.10.2015, C-362/14, *Schrems* vs. *Data Protection Commissioner,* ECLI:EU:C:2015:650; *Schrems II*, ECJ 16.07.2020, C-311/18, *Data Protection Commissioner* vs. *Facebook Ireland Limited and Schrems,* ECLI:EU:C:2020:559; see Mueller et al. in this volume). The subject of the legal dispute was the lawsuit filed by the Austrian Facebook user Schrems. He criticized the transfer of his personal data collected by Facebook to servers located in the USA because data protection was not adequately ensured. The basis for the data transfer was the so-called Safe Harbor Agreement between the EU and the USA. In 2000, the Commission certified that this agreement provided the USA with an adequate data protection level. However, the Safe Harbor Agreement only provided for a self-certification system by US companies; government authorities were not bound by it. Besides, the requirements of national security, public interest, and law enforcement took precedence over the Safe Harbor Agreement, so that US companies were obligated without restriction to interfere with the fundamental rights to respect for private life and the confidentiality of personal data. The ECJ overturned the adequacy decision (ECJ 06.10.2015, C-362/14, *Schrems* vs. *Data Protection Commissioner,* para 99, ECLI:EU:C:2015:650).

The ECJ ruled quite similarly in the *Schrems II* case. The EU Commission had determined in Decision 2016/1250 that the EU-US Privacy Shield ("Privacy Shield Decision") guarantees an adequate data protection level. The Court of Justice took a different view. The decision would, in turn, give undifferentiated priority to the requirements of national security, public interests, and compliance with US law and would not limit US surveillance programs to a strictly necessary minimum. Furthermore, no rights are granted to affected persons, so that there is again a violation of Article 7 and 8 CFR.

14.7 Conclusion and Future Outlook

The right to privacy encompasses a multitude of partial aspects of personality, which are also reflected at the legal system level. The constitutional order, including the law of the European Union and the European Convention on Human Rights, shows this complexity by protecting aspects such as the secrecy of personal data or the confidentiality of telecommunications as well as private life in general. The scope of protection is broad, but the question of the limits of fundamental rights must be asked each time anew and, because of rapidly changing threats, must also be redefined. Given the technical possibilities, the threat situation is tenser than ever. A wide range of information interventions are no longer the sole preserve of the state, which carries them out in the interest of the common good, but are also possible for private individuals. The state is therefore required more than ever to delimit the freedoms of individuals carefully. However, there are two main reasons why the private sphere is threatened in the sense of a self-determined way of life.

Those who want to participate in the blessings of the information society will not be able to avoid giving up parts of their private sphere. Those who consistently refuse to disclose their data will inevitably have to do without certain services (Berka, 2018, p. 760). Another threat is the market power that certain internationally active media such as Facebook have accumulated in recent years. As recent developments show, they are equally decisive in protecting privacy and freedom of expression (e.g., by blocking accounts). Bringing them under control is a challenge that can only be met through concerted international efforts (Berka, 2018, p. 761).

14.8 Exercise and Reflexive Questions

1. How do you rate your behavior? Do you tend to be generous or sparing with information from your private sphere?
2. Why is protecting privacy in the context of an employment relationship a particular challenge?
3. How do you assess the expansion of state surveillance instruments concerning the protection of privacy?
4. What is the state's role in protecting individuals from invasions of privacy by private third parties?
5. What do you think about cookie protection as companies and authorities currently implement it?

References

Berka, W. (2012). *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit. Verhandlungen des 18. Österreichischen Juristentages Linz 2012 (Band I/1)*. Manz.

Berka, W. (2018). Aktuelle Bedrohungen des Grundrechts auf Privatsphäre. *Österreichische Juristen-Zeitung ÖJZ, 2018*(1010), 755–762.

Berka, W. (2020). *Verfassungsrecht – Grundzüge des österreichischen Verfassungsrecht für das juristische Studium* (8th ed.). Verlag Österreich.

Berka, W., Binder, C., & Kneihs, B. (2020). *Die Grundrechte – Grund- und Menschenrechte in Österreich* (2nd ed.). Verlag Österreich.

Bezemek, C. (2016). *Grundrechte in der Rechtsprechung der Höchstgerichte*. Facultas.

Diehl, S., & Karmasin, M. (2013). Introduction. In S. Diehl & M. Karmasin (Eds.), *Media and convergence management* (pp. 1–5). Springer.

Diehl, S., Karmasin, M., Leopold, A., & Koinig, I. (2013). New competencies for the future: how changes and trends in media convergence demand new skills from the workforce. In S. Diehl & M. Karmasin (Eds.), *Media and convergence management* (pp. 353–376). Springer.

Eberhard, H. (2016). In Korinek, K., Holoubek, M., Bezemek, C., Fuchs, C., Martin, A., Zellenberg, U. (eds) Österreichisches Bundesverfassungsrecht – Kommentar. § 1 DSG.

Forgó, N., & Rieß, E. (2018). *Forgó, Grundriss Datenschutzrecht*. LexisNexis.

Grabenwarter, C., & Pabel, K. (2021). *Europäische Menschenrechtskonvention* (7th ed.). Verlag C. H.Beck oHG.

Jahnel, D. (2020). Datenschutzrecht. In D. Jahnel, P. Mader, & E. Staudegger (Eds.), *IT-Recht* (4th ed., pp. 521–576). Verlag Österreich.

Meyer-Ladewig, J., & Nettesheim, M. (2017). In J. Meyer-Ladewig, M. Nettesheim, & S. von Raumer (Eds.), Europäische Menschenrechtskonvention. Handkommentar (4th ed.). Art. 8 EMRK.
Öhlinger, T., & Eberhard, H. (2019). *Verfassungsrecht* (12th ed.). Facultas.
Pollirer, H.-J., Weiss, E., Knyrim, R., & Haidinger, V. (2019). DSG (4th ed.). § 1 DSG. Grundrecht auf Datenschutz. Status of update: 1.4.2019, rdb.at.
Riesz, T. (2019). In M. Holoubek & G. Lienbacher (Eds.), GRC-Kommentar (2nd ed.), Art. 8. Status of update: 1.4.2019, rdb.at.
Terlutter, R., & Moick, M. (2013). In S. Diehl & M. Karmasin (Eds.), *Media and convergence management* (pp. 163–176). Springer.
Wiederin, E. (2002). In K. Korinek, M. Holoubek, C. Bezemek, C. Fuchs, A. Martin, & U. Zellenberg(Eds.), Österreichisches Bundesverfassungsrecht – Kommentar, Art. 8 EMRK.
Wiederin, E. (2014). Schutz der Privatsphäre. In D. Merten, H. J. Papier, & G. Kucsko-Stadlmayer (Eds.), *Handbuch der Grundrechte – Grundrechte in Österreich* (pp. 363–418). C.F. Müller.

Doris Hattenberger is Assistant Professor at the Department of Law of the University of Klagenfurt. Her research areas concern IT law; environmental law; the European Union Law, especially in the field of economic policy; and university law. For further information, please see https://www.aau.at/rechtswissenschaften/oeffentliches-recht/team/hattenberger-doris/.

Florian Vidreis, LL.M. (WU) BSc is a former student assistant in the area of public law at the Department of Law of the Faculty of Management and Economics at the University of Klagenfurt with a research focus on fundamental and human rights law and media law. He currently works as an associate in the areas of Corporate/M&A and Banking & Finance at Fellner Wratzfeld & Partner. For further information, please see https://www.fwp.at/juristinnen/florian-vidreis.