2. Privacy from a Legal Perspective

Bart van der Sloot1

2.1. Introduction

This chapter adopts a 'Western' perspective, focusing on the United States of America, and in particular Europe. It will focus primarily, but not exclusively, on the informational aspect of privacy.2 Section 2 will discuss the role and function of privacy in the legal realm; it will engage with the origins of privacy in the legal realm, the way it is protected in both national and international legal orders and set out some general characteristics of the right to privacy. Section 3 will provide an overview of the most important legal principles; it will look specifically at the basis which underpins privacy in Europe and USA Section 4 will recount some of the traditional debates in legal research; such as whether people have the right to control or even sell their personal data. Section 5, discussing new challenges, will engage with the tensions between privacy protection and developments known as Big Data. Finally, section 6 concludes and provides some suggestions for further reading.

Before discussing the role of privacy within the legal realm, it is important to discuss five general characteristics of the legal realm itself. This section will discuss the notion of regulation, the regulator, norms, laws and fields of law.

1.1 What is regulation?

Without regulation, there would be anarchy. Most societies do not want anarchy, so they regulate. Regulation is based on norms. Law is one way to regulate. Laws are always the mitigating factor between fact and fiction, between practice and norm, between the situation that is (for example, a society in which there is violence and murder) and the desired situation (for example, a society in which no violence exists). Obviously, law is never fully successful in this endeavour. Although the legal regime provides that murder is prohibited (the norm), people still are being murdered (fact). To ensure compliance with the law, various tools of enforcement exist – these mostly depend on force (by the state). Consequently, the legal domain is always a combination of two elements:3 norm and force. Law enforcement can be achieved through various means, such as imprisonment, fines, naming-and-shaming, and capital punishment. Law has traditionally focused on retroactive forms of enforcement, that is, when a person violates the law she is sanctioned. There is a trend, however, to enforce the law proactively, that is before the law is violated. Methods employed to enforce the law proactively include imposing sanctions on people who are believed to pose a high risk to society

---

1 Thanks for Huw Roberts, Michael Collyer and Aviva de Groot for commenting on earlier drafts of this chapter.

2 A difference is often made between different types of privacy, such as bodily privacy, locational privacy (including the protection of the home), relational privacy (including the protection of family life) and informational privacy (including the protection of personal data and the secrecy of correspondence). Roessler 2005. Koops 2017

3 Derrida 1989.

(such as suspects of terrorism), by proactively steering behaviour of citizens (for example nudging in smart cities), by laying down codes of conduct, or by embedding law in technological code4 (for example, when online platforms simply block curse words, i.e. make it impossible to violate the norm). Law regulates citizens (natural persons), but also companies and other organizations (legal persons), including the state itself.

1.1.2 Who regulates?

Individuals as well as groups of people (family, friends) set norms. Organizations such as book clubs and companies have rules which may, for example, specify that an employee cannot arrive to work drunk. These forms of regulation and norm-setting are not, however, traditionally understood to fall under the legal regime. A law is seen as an instrument of the state or ruler (such as a dictator). It supposes a centralized form of order and authority. Within the state, the classical Western ideal is that there should be separation of powers.5 Before, in medieval Europe, the monarch commonly embodied every aspect of state power – he could make rules and laws, he acted as the head of the police and military and operated as the ultimate judge. Because this led to abuse of power, most states currently separate three powers in three different bodies: the law-making power (traditionally granted to the parliament, which ideally should have democratic legitimation), the executive power (the government), and the judicial power (the judges and courts).6

1.1.3 Who decides on norms?

One of the classical legal debates regards the question of whether all laws are man-made. So-called legal positivists stress that indeed they are, while proponents of natural law theories suggest that there are laws that are not man-made. The former stress that laws are the rules which are enforced by the executive power and that are generally followed by the population – they adopt a primarily descriptive stance.7 Natural law theories stress that there are laws that precede and supersede man-made law; these might either be the laws of God,8 or the laws derived from human nature.9 There is no uniform answer to the question of which natural laws or norms precede and supersede man-made laws, but reference is often made to legal principles such as human dignity, individual autonomy and personal freedom. Natural law theories provide the theoretical underpinning of human rights in the legal realm. Because natural rights are said to exist in the so-called state of

---

4 Lessig 1999.

5 Montesquieu 1989.

6 Obviously, there are exceptions and mixed forms. Referenda may take up part of the legislative process. Also, in many countries, the executive power has a big influence on the legislative process. The judiciary is often dependent in the sense that the members of the highest court are selected by parliament and/or the executive branch. And courts, and judges often engage in law-making.

7 Bentham 1970; Austin,1995; Hart 1994.

8 Aquinas 1914-1942.

9 Locke 1988.

nature (when there was no government and there were no man-made laws), they are believed to be intrinsic to being human.

The question inspired by the horrors of the Second World War is as follows: suppose a regime came to legitimate power and adopted laws, which on the one hand followed the correct constitutional procedures and had democratic legitimation, but on the other hand stated that all people of a certain religious denomination or with a certain ethnic background should be exterminated. Are those laws legal? Should citizens obey those laws? No, natural law theories would say, because there are higher laws than the man-made laws; if man-made laws contradict those, for example because they trample upon basic human dignity, they are simply null and void. In any democracy, a majority may rule over minorities; but there should be limits to the law-making capacities of the democratic majority.

The valid critique of the positivists is: who decides what these mystical, 'higher' norms are? Should judges decide on what higher norms exist and if so, what is their methodology for selecting them? If, on the other hand, these norms are selected through democratic means, how exactly do they differ from normal laws adopted by man? How is it that if these norms are supposedly innate to man (the claim of human or natural rights), that every region in the world has its own selection and interpretation human rights? In addition, they point to the fact that in the history of mankind, human rights have been violated more often than not. Are they really inalienable?

1.1.4 General characteristics of the law

Concerning man-made laws generally, there is no single doctrine on how laws should be adopted. Typically, democracies require a majority in parliament for adopting laws and qualified majorities (for example two-thirds of parliament) for adopting or amending constitutions.

There are certain general characteristics that have been ascribed to laws:10

Laws should be relatively stable, so that people know the rules and can take them into account (which becomes impossible if the norms change by the hour).

Laws should be proactive and not applied retroactively (a law adopted in May 2019, for example prohibiting wearing headscarves in public buildings, cannot be used to sanction a person that wore a headscarf in a public building in January 2019).

Laws should not ask the impossible of people (for example, a law simply stating 'citizens are prohibited from drinking water or other fluids').

A law should be general ('Jack Black cannot enter this building' is generally not considered to be a law; a rule saying 'People cannot enter this building' can be).

Laws should be publicized and generally accessible to the people.

The rules in the law should also be understandable (they need not be written in layman's terms, but generally understandable for people who want to).

Laws should not contradict each other.

---

10 Fuller 1969.

Laws should generally be enforced (if laws are not enforced, they are symbolic only).

1.1.5 Fields of law

There are four different fields law on a national level:

Civil law: regulates the dealings between citizens/companies among themselves. Examples are tort law, contract law, marital law, and consumer law.

Criminal law: also regulates the dealings between citizens and companies among themselves. Unlike civil law, which is seen as protecting the private interests of citizens and companies, criminal law is enforced by the state because the rules protect public interests. Public order provides the clearest example of this, with murder, rape, theft, and hate speech all prohibited.

Administrative law: procedural principles that regulate the bodies of the state and their dealings.

Constitutional law: the constitution is seen as the highest 'law' in a country (though not all countries have a constitution, for example the United Kingdom). It usually contains constitutional rights, such as freedom of speech and the right to privacy, and regulates the relationship between and dealings of the three branches of government (the legislative power, the executive power and the judicial power).

Typically, there are three types of courts in a country:

Lower Court: deals with a claim or a complaint in first instance. (In civil law cases, two private parties – citizens and/or private organisations - stand against each other. In criminal law cases, a private party – a citizen or an organisation - is prosecuted by the state. In administrative or constitutional law cases, a private party – a citizen or a private organisation – complains about the behaviour or a decision of the state. Civil law cases are called horizontal; criminal, administrative and constitutional cases are called vertical. Criminal, administrative and constitutional law is part of what is sometimes called public law, contrasting with civil law, which regulates horizontal relationships).

Court of Appeal: deals with appeals (either party may object to the decision of the lower court).

Constitutional Court/High Court/Supreme Court: deals with cases in final instance and can be the court of first instance for specific cases, such as those revolving around the constitutionality of laws (not all countries allow the high court to receive such cases). There is usually only one such court in a country; its decisions set precedents that should be followed by the lower courts and the courts of appeal.

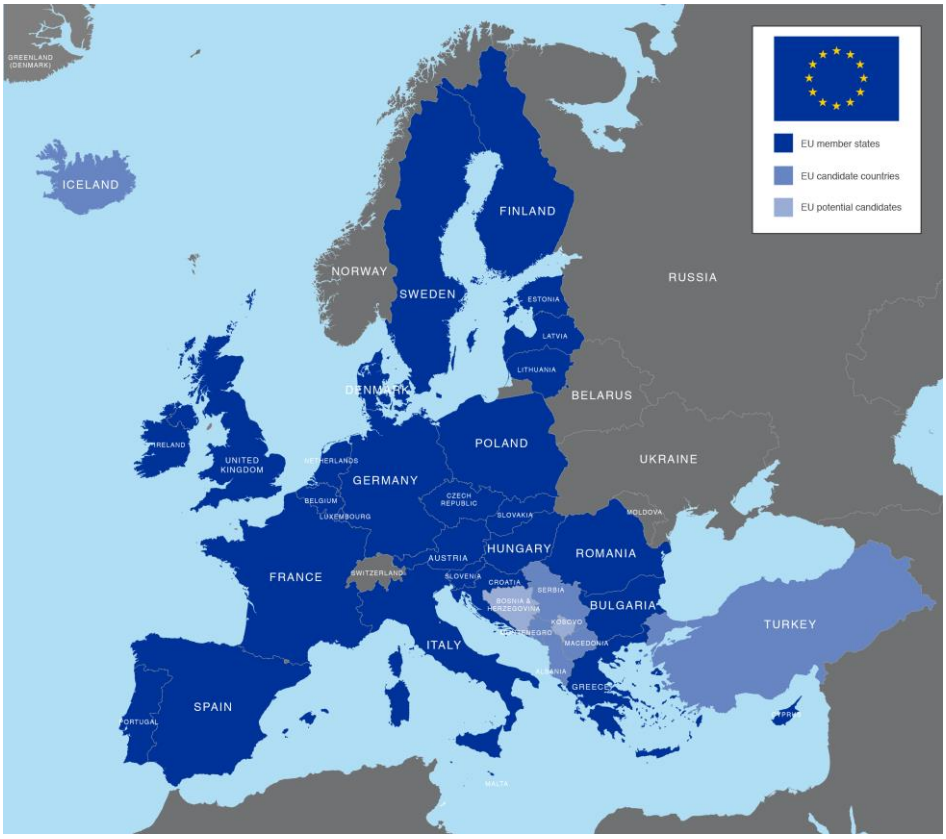
Then there are so-called human rights documents. These documents are perceived as higher than national laws and even constitutions. Some international courts overseeing those documents can invalidate national laws; citizens can appeal to these international courts even when their national supreme court has denied their request or delivered an unfavourable decision. Four prominent examples are:

Universal Declaration on Human Rights (UDHR) (1948) by the United Nations (UN) – no court oversees this document.

European Convention on Human Rights (ECHR) (1950) by the Council of Europe (CoE) – the European Court of Human Rights (ECtHR) oversees this document.

International Covenant on Civil and Political Rights (ICCPR) (1966) by the United Nations – is monitored by the United Nations Human Rights Committee.

Charter of Fundamental Rights (CFR) by the European Union (EU) (2000)11 – is monitored by the European Court of Justice (ECJ), like all regulation by the EU. The Charter can be compared to the constitution of the EU; the EU has competence to adopts laws on almost every aspect of society.



11 The CoE and the EU are different organizations. While 47 countries have ratified the ECHR (including countries such as the UK, Russia and Turkey), the European Union only has 28 members (27 when the UK leaves the EU). Traditionally, the difference between the two institutions was simple. The CoE regulated the field of human rights and the EU adopted legislation in the socio-economic area. However, the EU has entered the field of human rights realm as well, among others by adopting the Charter of Fundamental Rights. In principle, EU law and the decisions by the ECJ should take into account the standards contained in the ECHR and the jurisprudence of the ECtHR. Europe, as a continent, consists of about 53 countries.

Figure I: countries of the EU

Figure II countries of the Council of Europe (states that are yellow are the founding members; blue are the countries that joined the CoE later)

2.2. Meaning and function of privacy

This section will give a brief introduction into the role and function of privacy in the legal domain. Section 2.1 will recount the origins of privacy as a juridical concept; section 2.2 will introduce the forms through which privacy is protected in the national legal orders of a number of 'Western' countries; section 2.3 will give an overview of the most important privacy doctrines in human rights documents; and section 2.4 will discuss some of the general characteristics of the right to privacy and the right to data protection.

2.2.1 Origins of privacy in the legal realm

Privacy is perhaps the oldest legal principle. It pertains to the separation of the public and private domain. Where that boundary lies exactly differs from culture to culture, epoch to epoch, and country to country, but there always is one. In ancient times, the ruler or king had authority over the public domain, while the household fell under the rule of the pater familias, the male breadwinner of the family, who reigned over his family members like a king.12 The separation of the public domain from the private domain, meant that public laws, in principle, held no sway over the household. Privacy derives from private and the Latin privare, taking something out of the public domain, and is thus the exact opposite of publicare, taking something from the private to the public domain.13 A problematic consequence of the separation between the two spheres was that abuse of power by the father was mostly left unsanctioned – still until recently, rape within marriage was not a formal offence in a variety of countries.

The classical function of privacy was consequently to protect citizens from states entering the private domain. States held no sway over the household, or, in later time, could only enter the private domain for specific reasons and under certain conditions. Privacy was thus seen as an obligation of states not to abuse or overstretch their power; privacy protected citizens from totalitarian regimes.14 One of the classic theories to explain this principle is that in the state of nature, people were free and autonomous, but as there was no state, no law and no law enforcement, there was also notable violence between citizens (sometimes called a 'war of all against all').15 People then, so goes the hypothesis, decided to lay down their arms and give the state a monopoly of violence. The state had the power to adopt laws and enforce them; citizens could not use violence against each other. This 'social contract', however, only regarded the public domain, the domain where citizens interacted with each other, and not with respect to the private domain. Thus, the state had no or limited power to enter the latter domain.

2.2.2 National protection of privacy

12 Kantorowicz 2016.

13 Aries & Duby 1988.

14 Totalitarian, in this sense, refers to states that regulate society in its totality, including both the private and the public domain.

15 Hobbes 2006.

Besides the protection of the home and private land ('my home is my castle'), the right to privacy traditionally included bodily integrity, private communication (secrecy of letters), and the family life. To some degree, the protection of one's reputation and good name is also encompassed. Such types of protection have been incorporated in national constitutional orders ever since the 13th century. It is impossible to clearly demarcate the right to privacy from a legal perspective – in some countries, it includes the right to found a family, while in others this is not regarded a legal right. In some constitutions, it also includes bodily integrity, while in others, the inviolability of the human body is a separate doctrine. The same applies to the protection of reputation and other aspects of private life.

Besides constitutional rights, countries can protect privacy through various fields of law. For example, in civil law, businesses that gather personal information about citizens while misleading or mistreating them can be brought to justice through tort or consumer law. Privacy can also be regulated through criminal law: rape is an offence, so is entering a person's home without permission. Stalking is increasingly penalized, and in some countries, violating a person's reputation is sanctioned by criminal law.

Some selected examples of how privacy is protected in the constitutions of states are provided below. The Dutch and Italian constitution have different articles on different aspects of privacy, the German constitution contains a personality right, Spain has one longer article with paragraphs that protect several aspects of privacy, and the USA does not really have one specific article that is referred to for privacy protection (see in more detail section 3).

Dutch Constitution	German Constitution	Italian Constitution	Spanish Constitution	Amendments to the constitution of the USA
Article 10	Article 2 [Personal freedoms]	Article 13	Section 18	First Amendment
1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament. 2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording	1. Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law. 2. Every person shall have the right to life and physical integrity. Freedom of the person shall be inviolable. These	Personal liberty is inviolable. No one may be detained, inspected, or searched nor otherwise subjected to any restriction of personal liberty except by order of the Judiciary stating a reason and only in such cases and in	1. The right to honour, to personal and family privacy and to the own image is guaranteed. 2. The home is inviolable. No entry or search may be made without the consent of the householder or a legal warrant, except in cases	Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for

and dissemination of personal data.

3. Rules concerning the rights of persons to be informed of data recorded

concerning them and of the use that is made thereof, and to have such

data corrected shall be laid down by Act of Parliament.

rights may be interfered with only pursuant to a law.

such manner as provided by the law. In exceptional circumstances and under such conditions of necessity and urgency as shall conclusively be defined by the law, the police may take provisional measures that shall be referred within 48 hours to the Judiciary for validation and which, in default of such validation in the following 48 hours, shall be revoked and considered null and void. Any act of physical and moral violence against a person subjected to restriction of personal liberty shall be punished. The law shall establish the maximum duration of preventive detention.

of flagrante delicto.

3. Secrecy of communications is guaranteed, particularly regarding postal, telegraphic and telephonic communications, except in the event of a court order.

4. The law shall restrict the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.

a redress of grievances.

Article 11

Everyone shall have the right to inviolability of his person, without

prejudice to restrictions laid down by or pursuant to Act of Parliament.

Article 6 [Marriage – Family – Children]

1. Marriage and the family shall enjoy the special protection of the state.

2. The care and upbringing of children is the natural right of parents and a duty primarily incumbent upon them. The state shall watch over them in the performance of this duty.

3. Children may be separated from their families against the will of their parents or guardians only pursuant to a law, and only if the parents or guardians fail in their duties or the children are otherwise in danger of serious neglect.

4. Every mother shall be entitled to the protection and care of the community.

5. Children born outside of marriage shall be provided by

Article 14

The home is inviolable.

Personal domicile shall be inviolable. Home inspections, searches, or seizures shall not be admissible save in the cases and manners complying with measures to safeguard personal liberty. Controls and inspections for reason of public health and safety, or for economic and fiscal purposes, shall be regulated by appropriate laws.

Third Amendment

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

	legislation with the same opportunities for physical and mental development and for their position in society as are enjoyed by those born within marriage.		
Article 12 1. Entry into a home against the will of the occupant shall be permitted only in the cases laid down by or pursuant to Act of Parliament, by those designated for the purpose by or pursuant to Act of Parliament. 2. Prior identification and notice of purpose shall be required in order to enter a home under the preceding paragraph, subject to the exceptions prescribed by Act of Parliament.	Article 10 [Privacy of correspondence, posts and telecommunications] 1. The privacy of correspondence, posts and telecommunications shall be inviolable. 2. Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature	Article 15 Freedom and confidentiality of correspondence and of every other form of communication is inviolable. Limitations may only be imposed by judicial decision stating the reasons and in accordance with the guarantees provided by the law	Fourth Amendment The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

3. A written report of the entry shall be issued to the occupant as soon as possible. If the entry was made in the interests of state security or criminal

proceedings, the issue of the report may be postponed under rules to be laid down by Act of Parliament. A report need not be issued in cases, to be determined by Act of Parliament, where such issue would never be in the

interests of state security.

Article 13

1. The privacy of correspondence shall not be violated except in the cases laid down by Act of Parliament, by order of the courts.

Fifth Amendment

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a

2. The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorization of

those designated for the purpose by Act of Parliament.

Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Eleventh Amendment

The Judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted

against one of the United States by Citizens of another State, or by Citizens or Subjects of any Foreign State.

Fourteenth Amendment

Section. 1. All persons born or naturalized in the United States and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

2.2.3 Privacy in human rights documents

Human rights documents also contain the right to privacy. A distinction is sometimes made between the first wave of human rights documents, such as the Magna Carta from 1215, the second wave of human rights documents, such as the United States Bill of Rights and the French Declaration of the Rights of the Man and of the Citizen from the 18th century, the third wave of human rights documents, including the UDHR, the ECHR, and the ICCPR from the 20th century and the post 20th century documents, such as the Charter of Fundamental Rights, forming the fourth wave. Only in the third wave of human rights documents is the right to privacy explicitly mentioned; the older documents did contain prohibitions for states in relation to the abuse of power and conditions for entering the private domain, but this was not coined in terms of privacy. The first document that did was the UDHR, but even in there, the original title of the privacy provision was simply 'Freedom from wrongful interference'. Provided below are some of the most important examples of Human Rights documents that contain a right to privacy:

UDHR	ECHR	ICCPR	American Convention on Human Rights (1969)
Article 12 No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.	Article 8 Right to respect for private and family life 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the	Article 17 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.	Article 11 Right to Privacy 1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks.

	rights and freedoms of others.		
Article 16 1. Men and women of full age, without any limitation due to race, nationality or religion, have the right to marry and to found a family. They are entitled to equal rights as to marriage, during marriage and at its dissolution. 2. Marriage shall be entered into only with the free and full consent of the intending spouses. 3. The family is the natural and fundamental group unit of society and is entitled to protection by society and the State.	Article 12 Right to marry Men and women of marriageable age have the right to marry and to found a family, according to the national laws governing the exercise of this right.	Article 23 1. The family is the natural and fundamental group unit of society and is entitled to protection by society and the State. 2. The right of men and women of marriageable age to marry and to found a family shall be recognized. 3. No marriage shall be entered into without the free and full consent of the intending spouses. 4. States Parties to the present Covenant shall take appropriate steps to ensure equality of rights and responsibilities of spouses as to marriage, during marriage and at its dissolution. In the case of dissolution, provision shall be made for the necessary protection of any children.	Article 17 Rights of the Family 1. The family is the natural and fundamental group unit of society and is entitled to protection by society and the state. 2. The right of men and women of marriageable age to marry and to raise a family shall be recognized, if they meet the conditions required by domestic laws, insofar as such conditions do not affect the principle of nondiscrimination established in this Convention. 3. No marriage shall be entered into without the free and full consent of the intending spouses. 4. The States Parties shall take appropriate steps to ensure the equality of rights and the adequate balancing of responsibilities of the spouses as to marriage, during marriage, and in the event of its dissolution. In case of

dissolution, provision shall be made for the necessary protection of any children solely on the basis of their own best interests.

5. The law shall recognize equal rights for children born out of wedlock and those born in wedlock.

Article 18 Right to a Name

Every person has the right to a given name and to the surnames of his parents or that of one of them. The law shall regulate the manner in which this right shall be ensured for all, by the use of assumed names if necessary.

Article 19 Rights of the Child

Every minor child has the right to the measures of protection required by his condition as a minor on the part of his family, society, and the state.

African Charter on Human and Peoples' Rights (1981)

Article 18 1. The family shall be the natural unit and basis of society. It shall be protected by the State which shall take care of its physical health and moral. 2. The State shall have the duty to assist the family which is the custodian of morals and traditional values recognized by the community. 3. The State shall ensure the elimination of every discrimination against women and also censure the protection of the rights of the woman and the child as stipulated in international declarations and conventions. 4. The aged and the disabled shall also have the right to special measures of protection in keeping with their physical or moral needs.

EU Charter of Fundamental Rights

Article 3

Right to the integrity of the person

1. Everyone has the right to respect for his or her physical and mental integrity.

2. In the fields of medicine and biology, the following must be respected in particular:

– the free and informed consent of the person concerned, according to the procedures laid down by law,

– the prohibition of eugenic practices, in particular those aiming at the selection of persons,

– the prohibition on making the human body and its parts as such a source of financial gain,

– the prohibition of the reproductive cloning of human beings.

Article 7 Respect for private and family life

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

Article 8 Protection of personal data

Association of Southeast Asian Nations (ASEAN) Human Rights Declaration (2012)

19. The family as the natural and fundamental unit of society is entitled to protection by society and each ASEAN Member State. Men and Women of full age have the right to marry on the basis of their free and full consent, to found a family and to dissolve a marriage, as prescribed by law.

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Article 9 Right to marry and right to found a family

The right to marry and the right to found a family shall be guaranteed in accordance with the national laws governing the exercise of these rights.

2.2.4 Some general characteristics of the right to privacy and the right to data protection

This section provides some of the more general characteristic of the right to privacy and data protection. Especially, it will briefly reflect upon how these doctrines have changed over the last decennia.

It is important to underline three transitions with respect to the right to privacy:

Horizontalization: Privacy as a human and constitutional right was originally coined as a vertical right, which means that it regulates the relationship between the citizen and the state. However, there has been a trend of so-called 'horizontalization' of human rights (horizontal cases are between citizens and/or private organizations): in civil law cases, for example tort law or conflicts arising from consumer law, constitutional and human rights are taken into account.

Positive freedom: Privacy as a human and constitutional right was originally seen as a negative right, as freedom from interference (for example, protection against a government entering one's home), and not as a positive freedom, one that gives a right to engage in certain activities. Currently,

however, many of the privacy provisions are interpreted as also including positive rights, meaning a freedom to do something, such as the right to develop social relationships, the right to actively communicate with others and the right to develop one's personality to the fullest.

Positive obligation: Correspondingly, privacy as a human and constitutional right was originally seen as laying down a negative obligation for the state. The state had to abstain from abusing its power, while positive obligations require states to use their power in the best interests of the people. Currently, many privacy provisions in constitutions and human rights documents are interpreted in a way that states should also actively use their power to protect privacy (for example in horizontal relations) or to facilitate the personal development of its citizens.

The origins of the right to data protection lie partially in the data protection rules of northern European countries,16 which arose in several nations in the 1970s on the one hand, and the Council of Europe's Resolutions on data processing on the other.17 In parallel with this, data protection was emerging in the USA with the realization of the so called Fair Information Practices (FIPs), which were developed because the right to privacy was thought to be unfit for the 'modern' challenges of large automated data processing. The increased use of large databases (primarily by governmental organizations) raised a number of problems for the traditional concept of the right to privacy. First, data processing often does not handle private or sensitive data, but public and non-sensitive data such as car ownership, postal codes, number of children, etc. Secondly, and related to that, privacy doctrines at that time emphasized the right of the data subject as having an important role in deciding the nature and extent of her self-disclosure (which will be discussed in more detail in the next section).

However, because data processing often does not deal with private and sensitive data, the right to control by the data subject was felt undesirable. This is because governments need general data to develop, among other things, adequate social and economic policies. In addition, it was felt unreasonable, because in contrast to private and sensitive data, data subjects have no or substantially less direct and personal interest in controlling (partially) public and general information. Consequently, the term 'personal data' also included public and non-sensitive data, but instead of granting a right to control, the focus of data protection principles was on the fairness and reasonableness of the data processing.

Although data protection instruments were introduced to complement the right to privacy, early data protection instruments were explicitly linked to the right to privacy; the right to data protection was seen either as a sub-set of privacy interests or as a twin-right. As an example, the first frameworks for data protection on a European level were issued by the Council of Europe in 1973 and 1974. They regarded the data processing taking place in the private and in the public sector: the Resolution 'on the protection of the privacy of individuals vis-à-vis electronic data banks in the

16 Below is based on Van der Sloot 2014.

17 Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens (1973) <https://www.hsdl.org/?view&did=479784>.

private sector’18 and the Resolution ‘on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector’.19 Here, data processing issues are still explicitly seen as a part of as related to the right to privacy. The Resolution on the public sector also stated explicitly ‘that the use of electronic data banks by public authorities has given rise to increasing concern about the protection of the privacy of individuals’.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 by the Council of Europe did not contain the word privacy in its title but specified in its preamble:

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing; Reaffirming at the same time their commitment to freedom of information regardless of frontiers; Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples.

Also, Article 1 of the Convention, laying down the object and purpose of the instrument, made explicit reference to the right to privacy: ‘The purpose of this Convention is to secure in the territory of each Party [each member state to the Council of Europe] for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").’ Also, the explanatory memorandum to the Convention mentioned the right to privacy a dozen times.20 Thus, although the reference to privacy in the title was omitted, it is still obvious that the rules on data protection as laid down in the Convention must be seen in light of the right to privacy.

Gradually, however, the EU started to engage in the field of data protection and the European Union has traditionally adopted a different take on data protection. In the EU, data processing was partially treated as an economic matter, with the EU being the traditional guardian of the internal economic market, while the main focus of the Council of Europe has been to protect human rights on the European continent. The original mandate to regulate data protection by the EU was also found in market regulation. Still, however, in the rhetoric of the EU, the right to data protection was initially strongly connected to the right to privacy. This was also reflected in the Data Protection Directive from 1995, which makes reference to the right to privacy 13 times and in Article 1, concerning the objective of the Directive, holds: ‘In accordance with this Directive, Member States shall protect the

---

18 <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=58940 2&SecMode=1&DocId=646994&Usage=2>.

19 <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=59051 2&SecMode=1&DocId=649498&Usage=2>.

20 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca 434>.

fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.'

However, in the General Data Protection Regulation (GDPR) from the EU, which has replaced the Data Protection Directive as per May 2018, a radical choice was made. All references to the right to privacy have been deleted. Common terms such as 'privacy by design' have been renamed to 'data protection by design' and 'privacy impact assessments' have become 'data protection impact assessments'. Obviously, this is reflected on a higher regulatory level as well. In 2000, the European Union adopted a Charter of Fundamental Rights, which came into force in 2009. In it, the right to privacy and the right to data protection are separated and treated as two independent fundamental rights.

Besides the disconnection between the right to privacy and the right to data protection,

Just like with respect to the right to privacy, it is important to underline three general transitions with respect to data protection:

Increased scope: Data protection rules apply when 'personal data' are processed. More and more data is considered 'personal'. The sentence 'that person next to the garbage bin, with the black hat' can be considered personal data, even if the name or exact identity of a person is unknown. All data that relates to a person, or can be used to affect her, can be considered personal data. In addition, data which is currently not identifying anyone, but is likely to do so in the future can still be considered personal data. In the EU, there are even plans to regulate non-personal data.

Fundamentalisation: The two Resolutions of the Council of Europe merely recommended member states of the CoE to adopt rules to protect the principles contained in the Resolutions. They had a code of conduct or soft law like status. It was at the Member States' liberty to implement sanctions or rules regarding liability. Only in the Convention of 1981 was it explicitly provided that: 'Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.' Moreover, the Convention explicitly provided a number of rules regarding the application and enforcement of the rule on cross-border data flows, the cooperation between states and the national Data Protection Authorities. Adopting an EU-wide Directive in 1995 aimed at bringing uniformity in the national legislations of the different countries, which was promoted, among others, by providing further and more detailed rules for cross-border data processing. The member states of the EU were obligated to adopt the rules from the Directive in their legal order. As of May 2018, the GDPR has replaced the Directive. The fact that data protection rules are now contained in a 'Regulation' instead of a 'Directive' has important legal implications. A Regulation needs not be implemented by the member states of the EU – it has 'direct effect', which means that people and organisations can rely on the GDPR as such, while previously, they had to refer to the national implementation of the Directive. Finally, as has been stressed, in the Charter of Fundamental Rights, the EU has decided to make data protection a fundamental right of its own, next to such rights as privacy, the freedom of expression and the freedom from discrimination. The GDPR is seen as an implementation of article 8 of the Charter, which contains the fundamental right to data protection.

Juridification: Not only the material scope, but also the provisions in the instruments, providing the rights and obligations for the different parties involved with data processing activities, have extended quite significantly. The two Resolutions from 1973 and 1974 contained 8 and 10 articles respectively. The Convention from 1981 contained 27 provisions, the Directive 34 and the GDPR 99. While the two Resolutions were literally one-pagers, the Regulation consists of 88 pages.

2.3. Classic texts and authors

Discussing classic authors is a bit different for law than for most other academic disciplines. Law is made by legislators and partially by judges, not by scholars.21 Scholars reflect on legal texts and jurisprudence by courts. That is why this section will primarily refer to the legal texts and jurisprudence (which are called primary sources) and only marginally to texts by scholars (which are called secondary sources). This section briefly discusses the approach to privacy protection in the USA (section 3.1) and more thoroughly engages with the approach to privacy protection within the CoE (section 3.2), and the approach to data protection within the EU (section 3.3).

2.3.1 The protection of privacy in the USA

This section introduces three classic American authors (section 3.3.1), the most important privacy laws and rules (section 3.3.2), and five landmark cases of the American Supreme Court (section 3.3.3).

2.3.1.1 Classical authors

There has been a number of authors that had an effect on the development of privacy doctrines in the US. Three of the most important are:

Warren and Brandeis: arguably introduced the right to informational privacy in the US. They did so by distilling from existing doctrines and case law a new principle, namely the right to be ‘let alone’.

Prosser: distinguished between four types of tort that may be used for the protection of privacy, which were derived from the existing case law of various American courts. These are:

Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.

Public disclosure of embarrassing private facts about the plaintiff.

Publicity which places the plaintiff in a false light in the public eye.

---

21 Although this is a bit different for so called common law countries (such as the US, the UK, Canada, and Australia), which rely on judge-made law to a significant extent, than for civil law countries (such as most countries in Europe and Latin America) that rely predominantly on laws by parliament. In common law countries, there is more room for authors to develop new interpretations of rights and doctrines. The difference between common law and civil law countries is unrelated to the distinction between ‘civil law’, ‘criminal law’, ‘constitutional law’, etc.

Appropriation of the plaintiff's name or likeness.

Westin: wrote one of the first comprehensive books about informational privacy. He defined privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

2.3.1.2 Privacy laws

It is difficult to discuss the legislation of privacy in the USA because it is rather scattered. While in the EU, there is one general framework for data protection, and in the ECHR, there is one specific article on the right to privacy, this does not hold true for American Privacy Law.

2.3.1.2.1 The American Constitution

The First Amendment, providing the freedom to assembly and speech is sometimes invoked in privacy cases, when claims relate to positive privacy rights and freedoms.

The Fourth Amendment provides protection against arbitrary searches and seizures. It is seen as, inter alia, protecting the home of citizens against unlawful intrusion by the governement.

The Fifth Amendment provides procedural protection in criminal law cases, which may have an effect on the privacy rights of citizens.

The Ninth Amendment provides that enumeration in the constitution, of certain rights, shall not be construed to deny or disparage others retained by the people, such as possibly the right to privacy.

The Fourteenth Amendment provides protection to privacy rights to the extent they are related to due process.

2.3.1.2.2 Federal law

There have been several attempts to draw up omnibus privacy legislation in the USA. So far, however, these endeavours have been unsuccessful. That is why a patchwork framework exists of sectoral laws and privacy provisions for specific circumstances, five of which are:

The Federal Trade Commission Act: provides privacy protection in consumer relations and grants the Federal Trade Commission (FTC), the governmental body overseeing the sector, significant powers to enforce these provisions. The FTC is seen as the main governmental organization enforcing privacy in the USA.22

The Children's Online Privacy Protection Act (COPPA): regulates the online collection of information concerning children and is enforced by the FTC.

The Health Insurance Portability and Accountability Act (HIPAA): specifies rules for gathering and processing medical information.

---

22 Hoofnagle 2016.

The Fair Credit Reporting Act: regulates consumer-reporting agencies that use consumer reports or provide consumer-reporting information.

The Electronic Communications Privacy Act: contains rules for the interception of, inter alia, electronic communications.

2.3.1.2.3 Constitutions of States

Some constitutions of states contain a right to privacy, such as:

Article 1 of Alaska's constitution: 'The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section'.

Article 1 of the Californian constitution: 'All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy'.

Article 1 of Florida's constitution: 'Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law'.

Article 2 of the constitution of Montana: 'The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest'.

2.3.1.2.4 State law

Finally, there are privacy laws by states, which only apply on the territory of the state. Most important in this respect is the state of California, as most tech-companies are based there. An example is the California Electronic Communications Privacy Act.

2.3.1.3 Landmark cases

It is impossible to give a full overview of landmark cases by the Supreme Court on the right to privacy. Five influential cases are:

Olmstead v. United States (1928): concerned the use of wiretapped telephone conversations by the police without judicial approval. The use of the information obtained as evidence in a court case was declared not to be in violation of the Fourth and Fifth Amendment.

Griswold v. Connecticut (1965): concerned a Connecticut law that prohibited the use of, inter alia, contraception. The law was invalidated by the Supreme Court with a reference to 'marital privacy'.

Katz v. United States (1967): overturned the Olmstead case. Extended the notion of 'search' to include technological means of gathering evidence and underlined the doctrine of the 'reasonable expectation of privacy'.

Roe v. Wade (1973): on the basis of the 14th amendment, the Supreme Court accepted the so-called 'decisional privacy' doctrine, which grants women the right to decide over their own body, including the right to abortion.

Riley v. California (2014): concerned the warrantless search and seizure of a phone's content during an arrest. This was declared unconstitutional by the Supreme Court.

2.3.2 The European Protection of Privacy

Below is a discussion of the jurisprudence of the European Court of Human Rights (ECtHR) on Article 8 of the European Convention on Human Rights (ECHR). It is important to stress that although privacy is a human right, and even although human rights are the highest legal norms there are, legal rights are never absolute. Rights are subject to a double conditionality: first the conditions for the applicability of a right and second the conditions under which the right can be curtailed. This section will discuss in further detail two conditions for applicability, the concepts of ratione personae (section 3.2.1) and ratione materiae (section 3.2.2). Ratione personae refers to the question of personal scope – can the claimant indeed invoke the right she is relying on; for example, in most jurisdictions, a person cannot complain about the police entering the house of her friends uncle. Ratione materiae refers to the question of material scope – does the matter complained of fall under the protective sphere of the article relied on. For example, the fact that a person's car is stolen will normally not be considered a privacy violation. This section will also describe the conditions for curtailing the right to privacy (section 3.2.3). Finally, it will touch upon some of the landmark cases by the ECtHR (section 3.2.4).

2.3.2.1 Ratione personae

Three phases can be distinguished with respect to the doctrine of ratione personae under the European Convention on Human Rights: the original text of the ECHR, the interpretation of the Court roughly between 1960 and 2000, and the interpretation of the European Court of Human Rights after 2000. The doctrine of ratione personae sets limits to who can invoke a right to privacy.

2.3.2.1.1 Original text of the ECHR

The text of the Convention contains two modes of complaints: (1) inter-state complaints (for example Norway submits a case against Sweden for violating human rights) and

(2) individual complaints (for example, Mr Brown or Brown Bread Company submits a claim against Spain). The right to individual petition is open to three types of complainants: (2a) individuals, (2b) non-governmental organizations, and (2c) groups of individuals. Claims can only be brought against states. The focus originally was on inter-state complaints, as the ECHR was drafted against the backdrop of the Second World War. The core focus of the Convention was not to protect particular interest of particular individual claimants, but to prevent large and systematic abuse of power by states.

The Convention supervision consisted of a two-tiered system. First, the European Commission on Human Rights (ECmHR), which no longer exists today, would decide on the admissibility of cases and function as a filtering system. It was only with the Commission that the mechanism of individual

complaints existed. Even if a case was brought before the Commission by an individual complainant, and even if the Commission declared the application admissible, the applicant (natural person, legal person or group) had no right to submit it for review to the Court. This could only be achieved on initiative of the Commission or a Member State of the Council of Europe. The idea was that only those cases that transcended the mere individual complaint of an applicant, i.e. cases that concerned a large issue or a public interests, would be sent to the ECtHR. The ECtHR is the second tier; it deals with the cases in substance, and decides on the question of whether the Convention has been violated or not.

2.3.2.1.2 ECtHR's approach between 1960-2000

Over time, however, the Convention has been revised on a number of points so that, inter alia, individual complainants (individuals, groups, and legal persons) have direct access to the Court to complain about a violation of their privacy (the task of the Commission being reassigned to a separate chamber of the Court – the two-tiered system still exists). Moreover, over time, the Court has strongly emphasized individual interests and personal harm when it assesses a case regarding a potential violation of Article 8 ECHR, therewith transforming the ECHR from a document that was focussed on preventing large scale abuse of power by governments and protecting general and societal interests, into an instrument that mainly provided protection to the specific interests of an individual claimant. To give a few examples:

So-called in abstracto claims will in principle be declared inadmissible by the ECtHR. These are claims that regard the mere existence of a law or a policy, without them having any concrete or practical effect on the claimant.

A priori claims are rejected as well, as the Court will usually only receive complaints about injury which has already materialized. Claims about future damage will in principle not be considered.

Hypothetical claims regard damage which might have materialized, but about which the claimant is unsure. The Court usually rejects such claims because it is unwilling to provide a ruling on the basis of presumed facts.

The ECtHR will in principle also not receive an actio popularis, a case brought up by a claimant or a group of claimants, not to protect their own interests, but that of others or society as a whole.

According to the European Court of Human Rights, what distinguishes the right to privacy, under the interpretation of the ECtHR, from other rights under the Convention, such as the freedom of expression, is that it in principle only provides protection to individual interests. Cases that do not regard such matters, but mainly concern societal issues or public interests, are rejected by the Court when it regards Article 8 ECHR.

This focus on individual interests has also had an important effect on the types of applicants that are able to submit a complaint about the right to privacy. Although the Court has accepted that churches may invoke the freedom of religion (Article 9 ECHR) and that press organizations may rely on the freedom of expression (Article 10 ECHR), because Article 8 ECHR only protects individual interests, the Court has said that in principle, only natural persons can invoke a right to privacy.

The Court has rejected the capacity of groups to complain about a violation of human rights. Contrary to the intention of the authors of the Convention, it has stressed that only individuals who

have been harmed personally and significantly by a specific violation or infringement can bundle their claims.

Finally, the last non-individual mode of complaint under the Convention, the possibility of inter- state complaints, has had almost no significance under the Convention's supervisory mechanism. Although there are more than 20,000 judgements by the ECtHR on claims submitted under the Convention, less than 50 are the result of interstate complaints.

2.3.2.1.3 ECtHR's approach from 2000 onwards

Recently, however, the Court has been willing to relax its focus on the individual and individual interests somewhat and has allowed for occasional exceptions, for example:

The Court has been willing to allow for some twenty complaints by legal persons under Article 8 ECHR, inter alia when their business premises was searched by police officials without a warrant.

The European Court of Human Rights has been willing to provide protection to minority rights under the right to privacy; though not granting a right of a group to submit a claim, there are steps towards that direction.

In exceptional cases, the ECtHR has been willing to allow for in abstracto claims, in particular when there is a law that provides uncontrolled power to intelligence services to execute blanket mass surveillance programmes.

Such in abstracto claims can be seen as a priori claims, because no damage has yet materialized. The mere existence of a law or policy is addressed.

They may also be seen as shifting the focus from individual interest, towards general interests related to the abuse of power.

And they may be seen as a form an actio popularis, as these cases aim to protect the population at large.

2.3.2.2 Ratione materiae

The right to privacy under the ECHR has witnessed an significant extension in terms of its material scope. While the right to privacy was originally conceived as a quite narrow and limited doctrine, the ECtHR has extended its scope and meaning considerably. Article 8 ECHR is no longer interpreted as laying down negative rights for citizens only, it also includes many positive rights; it not only requires states to abstain from abusing their powers, but also to use them to certain positive ends. In general, Article 8 ECHR has provided protection to almost anything that is remotely related to the personal interest of the individual. Article 8 ECHR contains four elements of privacy, namely 'private life', 'family life', 'home', and 'correspondence'. Each of those terms has been interpreted in a very broad and all-inclusive manner by the ECtHR. In addition, the right to privacy has tended to overshadow some of the other provisions contained in the ECHR, such as the right to fair trial and the right to marry and found a family. Article 8 ECHR has been interpreted by the Court to include certain elements that were explicitly rejected by the authors of the Convention. And the ECtHR has brought

new rights and freedoms under the scope of the right to privacy that were not envisaged when the ECHR was drafted.23

Broadening of the terms in Article 8 ECHR:

Private life: Private live is perhaps the broadest notion under the European Convention on Human Rights. Although it was originally interpreted in narrow terms, relating to personal affairs in the private domain, it currently provides protection to almost every aspect of a person's life. The ECtHR has interpreted Article 8 ECHR as a very broad provision, that provides protection to a variety of matters, such as personal development, education, engaging in social relationships, and even the protection, at least under certain circumstances, from being fired at work (because the ECtHR holds that work is important for a person's development).

Family life: Again, although the notion of family life was originally only applied to the tradition family unit, over time, the ECtHR has extended this notion quite considerably. According to it, family life is a broad concept that may incorporate relations with aunts, nephews, grandparents, siblings, family in law, stepfamily, and may even relate to the relationship between a child and her legal representative or custodian. It not only provides the freedom from interference with those relationships, but also the positive freedom to develop such relationships.

Home: Although in its early case law, the European Court of Human Rights took a very traditional view on what falls under the concept of home, it now holds that a home is not only a house. The term may refer to any object in which a person lives. For example, under circumstances, a car may function as a person's home, if she sleeps in it. Interestingly, the Court has stressed that business premises may also fall under the concept of home, protecting companies against police searches.

Correspondence: Again, a same transition can be witnessed with respect to the term correspondence. According to the ECtHR, the term correspondence not only includes communication through traditional means, but also when use is made of modern technological devices or services, such as the internet. Consequently, Article 8 ECHR also provides protection to meta-data about communication over the internet.

Article 8 ECHR overshadows some of the other provisions in the ECHR, such as:

Right to marry and found a family: Article 12 ECHR provides: 'Men and women of marriageable age have the right to marry and to found a family, according to the national laws governing the exercise of this right'. This provision has been interpreted very restrictively by the Court, while Article 8 ECHR has been granted a very wide scope. Consequently, most issues relating to gay marriage, artificial insemination, adoption, and other non-traditional forms of marriage and procreation are dealt with under the scope of the right to privacy instead of Article 12 ECHR.

Right to a fair trial: The right to a fair trial is protected under Article 5 and especially Article 6 ECHR. Although these provisions are still highly influential and most cases under the ECHR relate to Article 6 ECHR, when issues of due process, procedural safeguards, and fair trial are related to privacy matters, the ECtHR is willing to discuss such elements under the right to privacy itself. Inter alia, it has stressed that it 'is true that Article 8 contains no explicit procedural requirements, but this is not

23 See for a full overview: Van der Sloot 2015.

conclusive of the matter. The local authority's decision-making process clearly cannot be devoid of influence on the substance of the decision, notably by ensuring that it is based on the relevant considerations and is not one-sided and, hence, neither is nor appears to be arbitrary. Accordingly, the Court is entitled to have regard to that process to determine whether it has been conducted in a manner that, in all the circumstances, is fair and affords due respect to the interests protected by Article 8'.24

The protection of reputation: Article 8 ECHR is based on Article 12 UDHR, which provides protection to one's reputation, besides the protection of private and family life, home and communication. This element was excluded from the scope of Article 8 ECHR by the authors of the Convention and moved to the second paragraph of Article 10 ECHR. Paragraph 1 of Article 10 ECHR grants the right to freedom of expression and paragraph 2, like paragraph 2 of Article 8 ECHR, provides for the conditions for limiting this right. Consequently, the protection of reputation was not intended as a subjective right of citizens, but as a ground on the basis of which governments could (and not must) limit the freedom of expression. Although the ECtHR has respected this principled choice for a long time, from 2009 onwards, the right to the protection of one's reputation, honour, and good name is currently said to fall under the scope of Article 8 ECHR, making it a subjective privacy right of citizens.25

Bodily integrity: A final example is the right to bodily integrity, which is not explicitly mentioned in Article 8 ECHR, although Article 2 (the right to life) and Article 3 (the prohibition of torture) do protect elements of one's bodily integrity. Still, the court usually turns to Article 8 ECHR when discussing issues relating to the body, such as medical procedures, mandatory vaccination schemes, and euthanasia.

Article 8 ECHR provides protection to freedoms explicitly left outside the scope of the ECHR, such as:

Right to property: The right to property was explicitly rejected from the ECHR.26 In addition, proposals to include under Article 8 ECHR the protection of private property were rejected during the

---

24 ECtHR, B. v. the United Kingdom, Application no. 9840/82, 8 July 1987, § 63-64.

25 A subjective right (droit subjectif) means that a person can invoke it. An objective right (droit objectif) is a legal principle that has general effect, but cannot be invoked by an individual claimant.

26 The ECHR only contains so called first generation human rights (not to be confused with the different waves of human rights. While first generation or civil and political rights require states not to interfere with certain rights and freedoms of their citizens in an arbitrary way (right to privacy, freedom of speech, freedom from discrimination), socioeconomic or second generation rights such as the right to education, to property and to a standard of living require states not to abstain from action, but to actively pursue and impose such freedoms by adopting legal measures or by taking active steps. The second generation rights were transferred to the 1th Protocol of the Convention, signing of which was non-mandatory. When the ECHR was drafted, the so called third generation rights, which revolve around intercultural and intergenerational solidarity, such as group rights, cultural rights and the right to a healthy living environment, did not yet exist. However, as will be explained below, the ECtHR has regarded the ECHR to be a so called 'living instrument', which means that it may be interpreted in present daylight. Consequently, the Court has provided protection to such third generation human rights by referring to existing provisions in the ECHR, in particular Article 8 ECHR. Reference can also be made to those tentatively describing the development of 'fourth generation human rights'. It does not matter whether reference is made to a right to general 'information management', the 'rights of indigenous peoples', the 'right to sustainable development

drafting process of the Convention. Still, the European Court of Human Rights has overturned that decision from the start and has consistently included the protection of private property under the scope of Article 8 ECHR, such as with respect to inheritance, destruction of private property, and even, as indicated above, the right to work.

Right to education: As with the right to property, the right to education was not included in the European Convention on Human Rights, but moved to an additional protocol, the signing of which was optional. Still, the ECtHR has included under the right to privacy, inter alia, the right of families to decide on the education of their children, for example in terms of language.

Personality rights: Although the UDHR contains several provisions that protect one's personality, these were left outside the scope of the ECHR because they were believed to be too vague and unspecific. Currently, however, Article 8 ECHR functions as a personality right – it provides protection to almost every aspect of a person's life, development, and flourishing.

Right to nationality: Although some of the other human rights documents do contain a right to residence, a right to nationality or a similar provision, such was excluded from the ECHR. The ECtHR has, however, included a right to residence in a certain country, or the prohibition to be expulsed, inter alia when such would have consequences for the family life of an immigrant (for example, a Tunisian immigrant has married an Italian woman, with whom she has children, but is threatened with extradition by the Italian government).

Article 8 ECHR is used by the ECtHR to include new rights and freedoms, that were not considered when drafting the ECHR, such as:

The right to data protection: Although the ECHR does not contain reference to a right to data protection, the ECtHR often refers to CoE's Convention from 1981, the EU Charter and other EU documents in this field. Although it does not provide a similar level of data protection to the EU, the Court has incorporated a number of elements traditionally part of the data protection regimes under the scope of the right to privacy.

The right to a clean and healthy living environment: Although the European Court of Human Rights does not accept a fully-fledged right to live in a clean and healthy living environment, it is prepared to deal with cases under Article 8 ECHR. This is true if the cases revolve around noise pollution, air pollution, scent pollution, and other forms of environmental damage, so long as the pollution affects the 'quality of life' of the applicant (which the Court agrees is a very vague and broad term).

Minority rights: states may be under the positive obligation to take active measures to respect and facilitate the development of minority identities. Like environmental rights, minority rights are not included in the European Convention on Human Rights. The Court, however, provides protection to both, with reference to the right to privacy.

Right to a name: a final example may be the right to a name and the right to change one's name. This right too is provided protection by the ECtHR with reference to Article 8 ECHR. It includes not only

---

of the future generation', 'women's rights, the rights of future generations, rights of access to information, and the right to communicate' or rights needed due to 'phenomena like the great developments in the area of biotechnology or the Internet'. Most, if not all, of these 'new' fourth generation human rights, suggested by different authors and commentators, would presumably, if accepted, be approached by the Court from the angle of Article 8 ECHR. Vasek 1977.

the right to alter one's first name or family name, but also to change one's identity, for example with respect to being transgender.

2.3.2.3 Conditions for curtailing the right to privacy

The previous two sections discussed two conditions for the applicability of the right to privacy: ratione personae and ratione materiae. There are a number of other conditions under the ECHR for the right to privacy to apply, but these are the most important ones. When the right to privacy applies, that is when it can be invoked by a claimant, the second question is whether there was a violation of this right in a particular circumstance. The right to privacy under the European Convention on Human Rights is a so-called qualified right.27 This means that Article 8 ECHR specifies under which conditions the right can be legitimately curtailed by the government; these conditions are listed in paragraph 2 of Article 8 ECHR, which specifies: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

Consequently, if the government infringes on a person's privacy, for example by entering her home, this need not be illegitimate or a violation of her privacy. The infringement can be deemed in harmony with the European Convention on Human rights when it abides by three cumulative requirements: (1) the infringement must have a legal basis; (2) must serve one of the legitimate goals as listed in the second paragraph of Article 8 ECHR; and (3) must be necessary in a democratic society. The ECtHR may find that although there has been an infringement of the right to privacy (as provided in paragraph 1 of Article 8 ECHR), this was a legitimate one and thus not in violation of Article 8 ECHR. The ECtHR only reaches this conclusion if all three requirements (legal basis, legitimate aim, necessary in a democratic society) have been fulfilled; if the government fails to fulfil either one of these requirements, a violation of the right to privacy will be found.

The Court may find that an infringement was not prescribed for by law for a number of reasons – the 'law', in this sense, is always the national law of a country. The ECtHR uses a quite wide definition of law, it includes not only legislation, but also judge-made law typical of common law jurisdictions and secondary sources, such as royal decrees and internal regulations. First, a violation of the Convention will be found on this point if the actions of governmental officials are not based on a legal provision granting them the authority to act in the way they did. Second, a violation will be established if the conditions as specified in the law for using certain authority have not been complied with, for example, if police officials have no warrant for entering the home of a citizen. Third, the actions of the governmental officials may be prescribed for by law, but the law itself may not be sufficiently accessible to the public. Fourth, the law may be so vague that the consequences of it may not be sufficiently foreseeable for ordinary citizens. Fifth and finally, the ECtHR has in recent years developed an additional ground, namely that the law on which actions are based does not contain sufficient safeguards against the abuse of power by the government. This typically applies to laws authorizing mass surveillance activities by intelligence agencies that set virtually no limits on their capacities, specify no possibilities for oversight by (quasi-) judicial bodies, and grant no or very limited rights to individuals, with respect to redress.

---

27 This sub-section is based on: Van der Sloot 2017B.

The Court may also find a violation of Article 8 ECHR if the infringement serves no legitimate aim. The second paragraph specifies a number of legitimate aims, primarily having to do with security related aspects, such as national security, public safety, and the prevention of crime and disorder. These terms are sometimes used interchangeably by the Court, but in general 'national security' is applied in more weighty cases than 'public safety', and 'public safety' in more weighty cases than the 'prevention of crime and disorder'. The right of privacy may also be legitimately curtailed to protect the rights and freedoms of third parties; for example, a child may be placed out of home (an infringement on the right to family life of the parents), because the parents sexually molested the child. The protection of health and morals may be invoked to limit the right to privacy, though this category is applied hesitantly by the ECtHR, because the protection of the morals of a country may lead to quite restrictive rules. Still with respect to controversial medical or sexual issues, such as euthanasia or BDSM, the ECtHR sometimes allows a country to rely on this ground to curtail the right to privacy. Finally, a country can rely on the 'economic wellbeing of the country'; this ground can only be found in Article 8 ECHR and in no other provision under the Convention. It is invoked by countries in a number of cases; for example, if an applicant complains about the fact that a factory or airport in the vicinity of her home violates her right to private life, the country can suggest that running a national airport is in fact necessary for the economic wellbeing of a country.

Much more can be said about the use, extent and interpretation of these aims, but this is unnecessary, because this requirement plays no role of significance. This is due to two factors. First, the ECtHR is often very unspecific about which term exactly applies, stressing that an infringement 'clearly had a legitimate aim', or that 'it is undisputed that the infringement served one of the aims as contained in Article 8 ECHR'. It often combines categories, underlining that the infringement served a legitimate aim, such as 'the prevention of crime', 'the economic well-being of the country' or 'the rights of others' or it merely lists all different aims and holds that one of these grounds applies in the case at hand. Furthermore, it introduces new aims, not contained in Article 8 ECHR, especially in cases revolving around positive obligations for states. Second, the Court almost never finds a violation of Article 8 ECHR on this point. It usually allows the government a very wide margin of appreciation with respect to the question of whether and which of the aims apply in a specific case and whether the infringement did actually serve that aim. In many cases, it simply ignores this requirement when analysing a potential violation of the right to privacy or incorporates it in the question of whether the infringement was necessary in a democratic society. Thus, only in 20 cases was Article 8 ECHR violated on this point.

Finally, the third requirement that must be fulfilled by a government wanting to curtail the right to privacy is that the infringement must be necessary in a democratic society. This question is approached by the Court primarily as a question of balancing the different interests at stake. 'This test requires the Court to balance the severity of the restriction placed on the individual against the importance of the public interest.'28 Consequently, to determine the outcome of a case, the Court balances the damage a specific privacy infringement has done to the individual interest of a complainant against its instrumentality towards safeguarding a societal interest, such as national security.

2.3.2.4 Landmark cases by the ECtHR

28 Ovey & White 2002, p. 209.

This chapter can not provide a full overview of the cases of the ECtHR on the right to privacy, as there are some 2,000 cases (second tier, meaning those cases that have been declared admissible) and more than 4,000 applications (first tier). Some of the most memorable cases include:29

Klass and others v. Germany (1978): The case concerned German legislation that allowed for the monitoring of citizen's correspondence and telephone communications without an obligation to inform them subsequently of the measures taken against them. Although the Court did not find a violation of Article 8 ECHR (the infringement was considered legitimate because the three conditions for limiting the right were met), it did stress that powers of secret surveillance of citizens are only allowed in so far as strictly necessary for safeguarding the democratic institutions.

P.G. and J.H. v. the United Kingdom (2001): The case concerned the recording of the applicants' voices at a police station. The Court stressed that the gathering of personal data fell under the scope of the right to privacy and found a violation of Article 8 ECHR because there was no legal basis for such data gathering.

S. and Marper v. the United Kingdom (2008): The case regarded the indefinite retention in a database of fingerprints, cell samples, DNA profiles, and similar data after criminal proceedings, even when suspects were acquitted. The ECtHR stressed that such a regime was disproportionate and consequently, could not be regarded as 'necessary in a democratic society'.

Delfi v. Estonia (2015): Central to this case was an Internet service provider that was held liable for user comments on its news website, because those violated the right to reputation of a person that was in the news. The ECtHR stressed that such a limitation on the freedom of speech was legitimate in light of the protection of the right to privacy (reputational harm).

Zakharov v. Russia (2015): The case concerned secret surveillance powers in Russia. There was no or limited judicial control on the use of power nor parliamentary control. The ECtHR allowed for an in abstracto claim and held Russia in violation of the Convention.

Szabó and Vissy v. Hungary (2016): The case regarded Hungarian legislation on secret antiterrorist surveillance. Like with Zakharov, the complaint was directed at the lack of control and checks and balances against the potential abuse of power. Again, the Court found a violation of Article 8 ECHR.

2.3.3 The European Data Protection Framework

This section will discuss the data protection principles by introducing the so-called Fair Information Principles (section 3.3.1), the rules contained in the EU General Data Protection Regulation (section 3.3.2) and some of the landmark cases by the EU Court of Justice (section 3.3.3). The focus is on the EU because it has the most elaborate and influential rules on data protection in the world

2.3.3.1 Fair Information Principles (FIPs)

The two classic texts on informational privacy are probably the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data from 1980 by the Organization for Economic Co-

29 www.echr.coe.int/Documents/FS_Data_ENG.pdf.

operation and Development's (OECD), an intergovernmental economic organization with 35 mostly 'Western' member states, and the previously mentioned in the CoE's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, from 1981. Those contain the so-called Fair Information Practices. The OECD guidelines mention eight:

Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

Purpose Specification Principle: The purposes for which personal data is collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle, except:

with the consent of the data subject; or

by the authority of law.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Openness Principle: There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle: An individual should have the right:

to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended.

Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

2.3.3.2 Rules contained in the GDPR

In the EU, the general data protection framework is provided by the General Data Protection Regulation. The GDPR replaces the Data Protection Directive from 1995. The GDPR will most likely have a worldwide effect (also called the Brussels effect), because of its large scope and broad requirements.

2.3.3.2.1 When does the GDPR apply?

There are five general conditions for the applicability of the GDPR.30

The activity must involve 'personal data', which is defined as: 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person'. As stressed, almost all data is or can be personal data.

This data must be 'processed', which is defined as 'any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'. Consequently, almost everything that can be done with personal data, such as storing, analysing, selling, and even correcting or deleting personal data, falls within the definition of 'processing'.

The rules in the GDPR apply primarily to the 'data controller' and partially on the 'data processor'. The data subject is the person who can be identified through the personal data. There is always a data controller and always a data subject; there may or may not be a data processor. The data controller is the natural or legal person who, alone or jointly with others, determines on the one hand the purposes and on the other hand the means of the processing of personal data. Simply put, the data controller is the person or organisation that decides that data should be processed and how. The controller is primarily responsible for upholding the data protection principles. The processor is the party that processes data on behalf of the data controller, for example a cloud provider that stores data on behalf of the data controller. The processor has to abide by a number of obligations of its own, but in principle, the data controller is responsible for the data processing by the data processor. If the latter makes a mistake, the former is responsible.

Obviously, the EU must have territorial competence for the GDPR to apply. There are four instances in which the EU claims competence:

When personal data are being processed in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

When data controllers or data processors are not established in the EU, but offer goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union.

---

30 Articles 1-4, 23, and 85-91 GDPR.

When data controllers or data processors are not established in the EU, but use personal data for monitoring the behaviour of EU citizens (for example by using cookies), as far as their behaviour takes place within the Union.

When an EU Member State has an embassy or similar organization outside the EU, that organization falls under the scope of the GDPR.

There are exceptions and limitations to the applicability of the GDPR, examples of which are:

When processing personal data is for a purely personal or household activity, such as keeping a list of telephone numbers and addresses of acquaintances.

Processing activities concerning national security (such as by secret services or intelligence agencies), over which the EU has no competence.

Processing takes place by EU institutions. The GDPR does not apply, but another Regulation does, which incorporates the same basic principles.

When processing activities take place by law enforcement authorities (such as the police). The GDPR does not apply, but a separate Directive (called the Police Directive) does, adopted at the same time as the GDPR. This Directive contains the same basic principles as the GDPR, but allows for more limitations and exceptions when this is necessary in terms of protecting public order and combating crime.

Then there are several fields in which the GDPR does apply, but for which Member States to the EU may make special arrangements, such as:

Freedom of expression;

Archiving purposes;

Scientific research;

Governmental transparency; and

Re-use of public sector information

If personal data are processed by a data controller and the EU has territorial competence and no exception applies, the GDPR will be applicable.

2.3.3.2.2 When is processing of personal data legitimate?

The GDPR contains its own version of the FIPs, specifying that personal data must be:31

processed lawfully, fairly, and in a transparent manner in relation to the data subject (‘lawfulness, fairness, and transparency’);

31 Article 5 GDPR.

collected for specified, explicit, and legitimate purposes (‘purpose specification’) and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’);

adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

accurate and, where necessary, kept up to date (‘accuracy’);

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’); and

processed in a manner that ensures appropriate security of the personal data (‘integrity and confidentiality’).

Each of these six basic principles must be respected; otherwise, the data processing will not be deemed legitimate. How these principles must be interpreted depends partially on the circumstances of the case.

The purpose specification principle requires a specific purpose to be designated before processing personal data. A specific purpose may exist, for example, when a pizza delivery service asks a customer for her address. An unspecific (and hence illegitimate) purpose are vague terms such as ‘improving customer experience’ or ‘innovation and product development’. Data may subsequently only be used for purposes directly related to this specific purpose. The pizza delivery service may also use the data to deliver hamburgers and perhaps, depending on the circumstances, send advertisements about new pizza deals. Nonetheless, it may not sell this data, for example, to a hotel, who then offers cheap vacations to the customer.

Only the data that is needed in relation to the specific purpose can be processed by the data controller. The pizza delivery service can ask for the address and a person’s name, but not her gender, political believes or sports interests. These are simply unrelated to and unnecessary for the purpose of delivering a pizza.

Data should be accurate and kept up to date. This is the responsibility of the data controller. Thus, if the pizza delivery service retains the address and name of a person, the next time the person orders a pizza, it is up to the pizza delivery service to ask whether the address has remained the same.

In principle, when the pizza is delivered, the pizza delivery service should delete the name and address of the customer. If it decides to store the name and address of a regular customer, it may only do so for a reasonable period of time. For example, if that person has not ordered a pizza for a consecutive six months, it might be reasonable to delete the data.

Finally, if personal data is stored by the data controller, it must ensure that these data are maintained safely and confidentially. This means that it must take measures to protect the databased from being hacked; in addition, data may be encrypted or pseudonymised, so that if data fall into the wrong hands, they are of no or little value to the that party. Also, the data controller must ensure that only those people within the organisation that need to access the personal data can do so and that others do not have permission or authorisation to enter the database (i.e. a need to know basis).

The GDPR gives further guidance on when data processing can be legitimate for three situations: (1) when personal data are being processed, (2) when so called ‘sensitive personal data’ are being

processed and (3) when personal data (sensitive or not) are transferred from the EU to countries outside the EU.

The GDPR exhaustively lists six grounds for processing personal data, one of which must apply for a processing initiative to be legitimate.

For sensitive personal data, the GDPR specifies: 'Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.' The general thought behind this provision is that because this data is so sensitive, they simply should not be processed. Still, 10 grounds are contained in the GDPR that provide an exception to this prohibition.

Finally, with respect to the transfer of personal data, the basic principle is that personal data should not leave the territory of the EU. This is because with the GDPR, the EU has laid down the highest standards for data protection in the world. Transferring the data to other areas would mean that the strict rules could be circumvented. That is why the GDPR holds that the data can only be transferred to a country outside the EU when more or less the same principles as contained in the GDPR are upheld. The GDPR provides three grounds on the basis of which there can be legitimate transfer:

When there is a so-called adequacy decision by the European Commission (which can be compared to the government of the EU), in which the Commission determines that a certain non-EU country, for example Switzerland, has an adequate level of data protection and data may be legitimately transferred to that country.

When there are appropriate safeguards. This means that not the country to which the data are transferred has an adequate level of data protection, but a specific organisation within that country has. This commitment is laid down, for example, in a contract between the EU-based organisation and the organisation based outside the EU, the latter receiving the personal data from the former.

For specific cases (for example when one file of one person is transferred to a country outside the EU), derogations may apply.

Six grounds for processing personal data32	Ten exceptions to the prohibition to process sensitive personal data33	Three grounds on the basis of which personal data (including sensitive data) may be transferred to countries outside the EU34
(1) the data subject has given consent to the processing of his or her personal data	(1) the data subject has given explicit consent to the processing of those personal	(1) Adequacy decision 'A transfer of personal data to a third country or an international organisation

32 Article 6 GDPR.

33 Article 9 GDPR.

34 Articles 44-50 GDPR.

for one or more specific purposes;	data for one or more specified purposes	may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.'
(2) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(2) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law	(2) Transfers subject to appropriate safeguards Appropriate safeguards can be achieved through either of the following means: 1. A legally binding and enforceable instrument between public authorities or bodies; 2. Binding corporate rules; 3. Standard data protection clauses adopted by the Commission 4. Standard data protection clauses adopted by a supervisory authority and approved by the Commission 5. An approved code of conduct 6. An approved certification mechanism 7. Subject to the authorization from the competent supervisory authority, contractual clauses between the controller or processor and the controller, processor, or the recipient of the personal data in the third country 8. Subject to the authorization from the competent supervisory authority, provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.
(3) processing is necessary for compliance with a legal obligation to	(3) processing is necessary to protect the vital interests of the data subject or of another natural person	(3) Derogations for specific situations

which the controller is subject;	where the data subject is physically or legally incapable of giving consent;	1. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards 2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; 3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; 4. the transfer is necessary for important reasons of public interest; 5. the transfer is necessary for the establishment, exercise, or defence of legal claims; 6. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; 7. the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. 8. When the transfer of personal data cannot be based on either of the exceptions above, the GDPR specifies: 'a transfer to a third country or an international organization may take place only if the transfer is not repetitive, concerns only a limited number of data

		subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data'.
(4) processing is necessary in order to protect the vital interests of the data subject or of another natural person;	(4) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious, or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;	
(5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(5) processing relates to personal data which are manifestly made public by the data subject;	
(6) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except	(6) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;	

where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This ground does not apply to processing carried out by public authorities in the performance of their tasks.

(7) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(8) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care, or treatment or the management of health or social care systems and services

(9) processing is necessary for reasons of public interest in the area of public health, such as protecting against

	serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices	
	(10) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes	

When processing personal data, the data controller must ensure that one of the grounds provided in the left column applies. If not, data processing will be considered illegitimate. When processing sensitive personal data, the same counts for the exceptions in the middle column. When transferring data from the EU to countries outside the EU, one of the grounds mentioned in the right column must apply for the transfer to be legitimate. If personal data are transferred, both a ground in the left and in the right column must apply. If sensitive data are transferred to countries outside the EU, both a ground in the middle and in the right column must apply. It is important to stress that these requirements come on top of the Fair Information Principles. Both the FIPs and the rules on legitimacy must be respected to be GDPR compliant.

It is often stressed that informational privacy or data protection is about informed consent or control over data by data subjects. This is untrue for the European legislation. A data controller can be fully GDPR-compliant without asking for consent a single time. Consent is one of the six grounds on which the processing of data can be based and only one of the 10 exceptions to the prohibition to process sensitive data. In addition, under the GDPR, the requirements for consent are tight to such an extent that it will be difficult to obtain legitimate consent from a data subject. Consent must be informed, specific, unambiguous and freely given. If privacy policies or terms and conditions are written in juridical jargon or are overly long, data subjects that consent will not be deemed to have been properly informed. Consent is thus invalid. If consent is given for broad and vague processing activities, such as ‘we process personal data for a variety of activities related to our services and in order to optimize customer experience’, consent will not be deemed to be specific. If consent is given as part of a larger contract, in which the data subject gives consent to a variety of matters, consent will not be deemed to be given unambiguously. When consent is mandatory for a data subject to enter a site or service, consent will not be deemed to be given freely. And even if all these conditions are met, the data subject may always revoke its consent. Finally, it is important to note that consent cannot be used to curtail the FIPS. If the data subject consents, for example, to the processing of more data than the data controller strictly needs to fulfil its goal, it still conflicts with the data minimisation principle and hence is a violation of the GDPR.

Consent	Conditions for consent35	Conditions applicable to child's consent in relation to information society services36
‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;37	Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.	Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this	If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.	The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

35 Article 7 GDPR.

36 Article 8 GDPR.

37 Article 4 GDPR.

context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.38

It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.39

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

Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Children merit specific protection with regard to their personal data, as they may be less aware of the risks,

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the

38 Recital 32 GDPR.

39 Recital 33 GDPR.

consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.40

Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (1) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing

performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

40 Recital 38 GDPR.

for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.41

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.42

2.3.3.2.3 What additional obligations do data controllers have?

Data controllers have to respect the FIPS, have to obtain a legitimate ground for processing personal data, sensitive data or transferring them and have to abide by a number of more specific requirements provided below. There are conditions for and exceptions to each of those obligations;

41 Recital 42 GDPR.

42 Recital 43 GDPR.

these are too detailed to describe here. Instead, the basic requirements are provided. There are six mandatory requirements:43

The GDPR introduces a general obligation for data controllers to keep records of their processing activities, in which they describe meticulously what data they have, about whom, for what reasons they are processed, with whom they are shared, etc.

The GDPR requires data controllers to demonstrate transparency regarding their processing activities. They should provide data subjects (on their own initiative) with the information about the data processing activity, e.g. what data is processed about the data subject, why, by whom, how long it will be processed, which technical and organisational safety measures have been adopted, etc.

There must be appropriate technical and organisational safeguards applicable to the processing of personal data. Such security measures can include pseudonymization, encryption and protecting databases against hackers. Such organisational measures may include introducing authentication systems for entering databases, limiting access-rights to a small number of people within the organisation and logging which employees have entered databases and when.

The GDPR requires a data controller to notify the relevant Data Protection Authority (DPA – its role is explained in more detail below) when there has been a data breach (data has fallen into the hands of third parties, for example hackers, has been accidentally lost, or someone within the organization has had unauthorized access) and the data subject has to be informed when the data breach is likely to affect her.

A Data Protection Officer (DPO) must be appointed by public authorities processing data and by private organizations when they are processing sensitive data, systematically monitoring citizens on a large scale or perform other risk-prone processing operations. A data protection officer has the responsibility to ensure that the data protection principles are respected within an organization. The officer has an independent position and should be fully equipped by the organisation to allow her to assess to what extent the organisation is GDPR-compliant and what measures should be adopted to ensure compliance.

When there are risk-prone processing operations, an organization has to perform a so-called Data Protection Impact Assessment (DPIA), in which it assesses the impact of its intended data-processing operation. It has to adopt precautionary measures to mitigate risks when they follow from such an Impact Assessment. When the risks cannot be mitigated, the data controller should abstain from its intended data-processing operation or ask the DPA for permission.

In addition, there are two optional clauses in the GDPR:

There is no obligation, but a possibility for data controllers to draw up a code of conduct. A code of conduct is a primarily sectorial instrument, which specifies in further detail how the principles in the GDPR should be interpreted in specific contexts/sectors. If an association (e.g. the association for European universities) has adopted such a code of conduct (which is in itself optional), all members

43 Articles 24-43 GDPR.

of that association (e.g. the specific universities being member of the association for European universities) are obliged to abide by the rules in the code of conduct.

The GDPR promotes, but does not oblige, self- and co-regulation through self-certification. A certificate can only be given to an organisation by an officially authorised certification body. A certificate may, for example, state: 'This organisation has adopted sufficient organisational and technical security measures to be, on this point, GDPR-complaint'.

2.3.3.2.4 What are the rights of data subjects?

Data subjects have rights, which the data controller (and the data processor to some extent), needs to respect.44 Most of these rights correlate with the obligations of the data controllers. Thus, only if the data controller ignores its duties, which is a violation of the GDPR in itself, will the data subject have a legitimate reason to invoke its rights. The right to information of the data subject correlates with the obligation of the data controller to provide data subjects with information on its own behalf. The right to rectify personal data of the data subject correlates with the obligation of the data controller to keep data correct and up to date. The right to erasure (sometimes called the right to be forgotten) by the data subject can only be invoked when the data controller is processing data illegitimately. The right to object to the processing of data only applies when the data controller has no legitimate ground for processing the data. And finally, the right of the data subject not to be subjected to autonomic decision making, including profiling, is in fact an obligation of the data controller not to make decisions without human assessment, at least when the decision affects the data subject significantly.

Consequently, if the data controller follows the rules of the GDPR, data subjects will not have a legitimate claim to any of their rights. There are two exceptions: rights that do not correlate with independent duties of the data controller, which can be invoked by the data subject even if the data controller has not violated any obligations under the GDPR. (1) The right to copy gives the data subject the right to not only request information about the data that is being processed about her, but also a right to obtain a copy of that information. This is especially important in the medical sector. (2) The right to data portability, which only applies when data subjects have given personal data to a data controller (e.g. Facebook) themselves and when the ground for processing this data is the consent of or a contract with the data subject (e.g. 'I agree to be on Facebook under the following conditions'). When a person decides to leave the data controller (e.g. leaves Facebook in order to join another social network), the data subject can take the data that she has provided with her or ask the data controller to send the data to the new data controller she is going to (right to data portability).

2.3.3.2.5 How are the rules in the GDPR enforced?

If the data protection rules are not followed by the data controller, and the data protection officer has been unable to correct the situation, the data subject may submit a complaint to either a judge or to the DPA. The DPA is a governmental agency that has a variety of tasks; it can be compared to a market regulator, such as exist in inter alia the telecommunications sector. The DPA can also take measures on its own initiative, that is without the complaint of a data subject. The DPA will in

44 Articles 12-22 GDPR.

principle only take action when the data controller has neglected its obligations as specified in the GDPR.

A general problem with data protection provisions before the introduction of the GDPR has been that they have lacked adequate enforcement. This is tackled by the GDPR, in particular in five ways:45

A general problem was that the EU Data Protection Directive 1995 needed to be implemented by each Member State. This meant that there existed differentiation in the rules among countries. Data controllers were often established in countries where the rules applicable to its business endeavours would be least strict. This is addressed by the GDPR because a Regulation, as opposed to a Directive, has direct effect throughout the EU. This means that data subjects can rely directly on the GDPR, without having to refer to the national implementation of the EU rules (as was the case with the Data Protection Directive).

A general problem was that the enforcement of the data protection rules was mostly in the hands of national governments and the Data Protection Authority, which each country needed to install. However, countries differed in their approach to enforcement, some being more lenient than others. Again, data controllers were often established in countries were the level of enforcement was low. Under the GDPR, there is enhanced cooperation between the different DPAs and one DPA can be assigned authority over a company with respect to its establishments and activities throughout the whole EU.

In addition, there are several ways for the European Commission and other EU institutions, such as the European Data Protection Board, in which all national DPAs have a seat, to engage in monitoring and norm-setting, to further harmonize regulation and provide more specific provisions on data-processing activities.

Not all DPAs were well equipped prior to the GDPR; some of them were also lacking independence from the government. The GDPR guaranties the independence of DPAs and gives them wide authority on a number of accounts.

Finally, a general problem has been that the fines that could be imposed on companies that violated the data protection principles were considered low, especially when considering the high profits made by tech-companies. The GDPR addresses this problem and allows for sanctions that may run up to 20 million euro or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

2.3.3.5 Landmark cases by the ECJ

It is impossible to give a full overview of the case law of the ECJ on the right to data protection. Instead, four recent and influential cases will be briefly touched upon:

45 Articles 51-84 and 92-93 GDPR.

Digital Rights Ireland (2014): Concerned an EU Directive which required states to retain data for a period of time on, inter alia, citizen's Internet use. The ECJ rendered this Directive invalid, because it was considered an illegitimate infringement on the rights to privacy and data protection.

Google Spain (2014): Concerned the request of a citizen about whom compromising information could be found by using Google's search engine. The Court ruled that there may be an obligation of an operator of a search engine to remove from the list of results links to web pages, published by third parties, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, when its publication in itself on those pages is lawful.

Schrems (2015): Concerned an adequacy decision (known as 'Safe Harbour') of the European Commission in which the United States of America was considered, with respect to some data-processing operations, to provide an adequate level of data protection. The ECJ declared that decision invalid, because it was not convinced that the US did have an adequate level of protection.

Tele 2 (2016): Concerned the EU e-Privacy Directive and the obligation to retain data about, inter alia, Internet traffic. The ECJ stressed that the rights to privacy and data protection preclude national legislation which provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

2.4. Traditional debates and dominant schools

As stressed before, scholarly debates are less important in law than in most other fields of research. There is some discussion, but these mainly stem from the differences in legal regulation of privacy in various countries and jurisdictions. Below a brief introduction to five of those discussions.

2.4.1 Privacy as control

Some authors feel that privacy and data protection are about control of the individual, either over her data, or, for example, control over who has access to the house. This school mainly focuses on individual rights and individual interests mainly. It presupposes that the individual can practically take control over her privacy and personal data. In part, this school is inspired by the so-called census decision by the German Constitutional Court, who has introduced the notion of 'informational self-determination'.46

Others stress that privacy and data protection are in essence not individual rights that protect individual interests, but obligations of states and data controllers not to abuse their powers and/or to use their powers in a good and careful manner. Privacy and data protection, in this school, are seen as only partially protecting individual interests, and mainly focussed on the public interest. Furthermore, scholars have pointed to the fact that individuals are simply unable to control their data, because there are simply too many data-processing initiatives that contain one's personal data.

46 Bundesverfasungsgericht 15 December 1983.

2.4.2 Privacy as property

In addition to seeing privacy and data protection in terms of individual control, a few scholars have argued that people should have a property right over their personal data. Seeing that large companies make high profits by gathering, processing, and selling personal data or profiles distilled from those data, scholars have argued that property rights over personal data may be introduced, so that individuals could at least have a share in the profits that are being made by using their data.

Others stress that it is impossible to give property rights over personal data to individuals. Personal data are all data, also data that can be gathered by walking in the street – 'that man with the black shawl' may be considered 'personal data'. It is simply undoable to restrict the use of these types of data by subjecting them to property rights. In addition, why would anyone be legitimized to claim a property right over information like 'man' or 'black shawl'? Finally, some scholars stress that if there are personal data that can be seen as so intrinsic to a person's identity or personality that she should have a right of control, then it would be simply unethical to treat these as an economic and 'tradable' good. A person just cannot sell herself into slavery, because the body is not a transferable good that can be owned by another - personal data shouldn't be traded either.

2.4.3 Privacy as a personality right

Some stress that privacy should be seen as a personality right. They point to the German constitution, in which a personality right is firmly engrained, and to the trends in the various jurisdictions, such as the case law of the European Court of Human Rights, under which the right to privacy has been transformed into such a personality right. They point to the fact that personality rights have a bigger material scope and thus provide for more protection and grant more freedom to citizens.

Others point to the fact that the bigger a right or doctrine is, in general, the weaker it becomes. By including all types of remotely related interests under the same doctrine, more exceptions and limitations will be necessary. In addition, some scholars stress that privacy and personality rights are simply two different doctrines that should not be mixed up. Privacy rights are about 'freedom from', while personality rights concern the 'freedom to'.

2.4.4 Privacy and data protection

There is discussion about whether there is a difference between privacy and data protection or not. For many American scholars, the protection of personal data falls under the scope of informational privacy. Some feel that the European scope of the notion of 'personal data' is too broad, others feel that the obligations on data controllers are too strict and place too many hurdles for innovative companies and start-ups that base their business models on the processing of personal data.

For many European scholars, however, there is a clear distinction between privacy rights and data protection principle - although within the Council of Europe laws and jurisprudence, this distinction is less strict than in the European Union. Many scholars around the world have praised the General Data Protection Regulation as an attempt not so much to protect the privacy of citizens, but to curtail

the gathering and processing of data by companies and other organizations, and the growing power and information imbalances that this entails. The GDPR is seen as a highly 'proceduralistic' instrument, to the dismay of some, while being lauded by others. In any case, to many Europeans, data protection legislation is of a different nature than privacy laws: they have different scopes, different obligations, rights and different approaches (as explained in section 3.2 and 3.3 of this chapter).

2.4.5 Balancing

As has been stressed, one of the most common methodologies used by courts, but also politicians and researchers, to determine the outcome of a case or a conflict between doctrines and principles is 'balancing'. Through this methodology, one right or principle is balanced against the other, for example the right to privacy against the right to freedom of speech or individual autonomy against national security. The outcome is determined on a case-by-case basis, by weighing one interest against the other, taking account of the circumstances of the case.

Others have argued that balancing is a nonsensical metaphor in the legal realm. Privacy has no weight, nor does security. There is no objective methodology of weighing and there is no base unit (such as a kilogram) to express weights of legal principles. Still others have underlined that when applied in privacy cases, it normally means that privacy is outweighed by security, because privacy is limited to an individual interest, while security, so it is said, relates to the interests of the entire population.

2.5. New challenges and topical discussions

There are many challenges and topical discussions concerning the rights to privacy and data protection in the legal realm. Mostly, they relate to new data surveillance techniques, smart applications, and the internet of Things (IoT). Big Data is the overarching term that is used to describe many of the societal, economic, and technical changes, such as the technical capacity to gather data in all types of structures, the reduced costs of storing and analysing data, and the interest of many companies and governments to apply data-driven innovation. It is impossible to give an exact definition of Big Data, but in general it is described as an asset with the following affordances (in how far these are real is a matter of debate): large quantities of data that can be gathered without a concrete or specified reason. These data will subsequently be analysed to see which data is valuable, and computer algorithms can find patterns and distil correlations that go beyond human hypotheses. Data can be reused for new purposes and combined with existing databases, offline or online, or complemented with data from open sources, for example by scraping the Internet. By analysing large quantities of data, statistical correlations may be found and group profiles can be developed. It is obvious that this trend will conflict with a number of principles of the current privacy and data protection regime. Three examples will be provided. Section 5.1 will discuss data protection principles in light of Big Data developments, section 5.2 will analyze the focus on the individual in the current legal framework and section 5.3 will discuss legal regulation as such in light of recent technological developments.47 Section 5.4 will provide a brief discussion.

47 These sections are partially based on: Van der Sloot and Van Schendel 2016.

2.5.1 Big Data challenges to Data Protection principles

Personal data must be collected for specified, explicit, and legitimate purposes, while Big Data and new data technologies enable the indiscriminate gathering of personal data.

Personal data may not be further processed in a way that is incompatible with the original purpose, while the key adage of Big Data is that data can always have a second life and be reused for purposes previously unforeseen.

The current data protection regime is based on the principle of data minimization, while the trend with Big Data technologies is rather to collect as much data as possible and store it for as long as possible.

Under the legal framework, data should be treated confidentially and should be stored in a secure manner, while this principle is challenged because data is increasingly shared between different organizations and/or made available online (open data).

The current framework also specifies that the data should be accurate and kept up to date. It is, however, becoming less and less important for data analytics to work with correct and accurate data about specific individuals, because the correlations found and group profiles made transcend the individual. A general correlation or group profile can be distilled from messy data sets. 'Quantity over quality of data', so the saying goes.

Data subjects have the right to request information about whether data relating to them is processed, how, and by whom. This principle is also at odds with the rise of Big Data, partly because data subjects often simply do not know that their data are being collected and are therefore not likely to invoke their right to information. This applies equally to the other side of the coin: the transparency obligation for data controllers. For them, it is often unclear to whom the information relates, where the information came from, and how they could contact the data subjects, especially when the processes entail merging different databases and the reuse of information.

Consequently, Big Data challenges many of the classic Fair Information Principles and Data Protection principles.

2.5.2 Big Data and the individual

The current privacy and data protection paradigm focuses to a large extent on the individual, on subjective rights, and personal interests. This is put under pressure by new data technologies.

The principle of ratione personae seems hard to maintain in Big Data processes, because these processes do not focus on specific individuals, but on large groups of people or potentially everyone. Briefly put, many Big Data processes and applications based thereon are general, large-scale projects that have an impact on big groups or on society as a whole, while the link to individuals and individual interests is increasingly vague and abstract. The problem with large scale data processing activities, such as data gathering by intelligence agencies, is not so much that a specific individual is affected, but that communication data are intercepted about thousands or even millions of people. It regards a structural and societal problem.

The principle of ratione materiae is also challenged in Big Data processes because it is increasingly unclear whether a particular right is at all involved with a certain practice. To give an example, the application of data protection instruments depends on whether personal data are processed. However, increasingly, data is no longer stored and processed on the individual level; rather, the trend is to work with aggregated data and to generate general patterns and group profiles. These statistical correlations or group profiles cannot be qualified as personal data, but can be used to change the environment in which people live significantly. An individual as part of a group or as assigned to a particular category may not be identifiable directly herself, but can nonetheless be affected by the data processing.

The current legal system places much emphasis on subjective individual rights. The question is whether this focus can be maintained in the age of Big Data. It is often difficult for individuals to demonstrate personal injury or an individual interest in a particular case; individuals are often unaware that their rights are being violated or even that their data has been gathered. In the Big Data era, data collection will presumably be so widespread that it is impossible for individuals on a practical level to assess each data process to determine whether it includes their personal data, if so whether the processing is lawful, and if that is not the case, to go to court or file a complaint.

Consequently, the focus on privacy as an individual right providing protection to individual interest is put under pressure by Big Data innovations.

2.5.3 Big Data and legal regulation

Finally, Big Data and other modern data technologies challenge the legal regulation of privacy. This is because law is always dependent of legally defined categories and concepts, which are becoming increasingly blurry and vague in the age of Big Data. Examples are:

Data processing is becoming increasingly transnational. This implies that more and more agreements must be made between jurisdictions and states. Making these agreements legally binding is often difficult due to the different traditions and legal systems. Rapidly changing technology means that specific legal provisions can easily be circumvented and that unforeseen problems and challenges arise. The legal reality is often overtaken by events and technical developments.

The fact that many of the problems resulting from Big Data processes predominantly revolve around more general social and societal issues makes it difficult to address the Big Data issues within specific legal doctrines, which are often aimed at protecting the interests of individuals, of legal subjects. That is why more and more national governments are looking for alternatives or additions to traditional black letter law when regulating Big Data – for example self-regulation, codes of conduct, and ethical guidelines.

The legal framework often depends on static concepts and divisions. These are put under pressure by Big Data processes. For example, the current legal regime is based on different levels of protection for different types of data. Article 8 ECHR protects private data (which do not necessarily have to be sensitive) and sensitive data (which do not have to be private) and provides limited protection only to other personal data and metadata. The GDPR distinguishes between ordinary personal data, sensitive personal data, anonymous data (which fall outside the scope of the GDPR), and pseudonymous data. However, it is increasingly questionable whether these distinctions are still

tenable in the age of Big Data. Increasingly, these categories are merely temporary stages, because data can almost always be linked back to an individual or can be de-anonymized or re-identified. Overall, while the current legal system is focused on relatively static stages of data and links to these stages a specific protection regime, in practice, data processing is becoming a circular process: data are linked, aggregated, and anonymized and then again de-anonymized enriched with other data in order to create sensitive profiles, etc.

In conclusion, the possibility of protecting privacy through legal means is put under pressure by the developments known as Big Data.

2.5.4 Discussion

There is discussion about what these challenges should mean for the legal regulation of privacy and data protection. In general, several positions can be distinguished, five of the most influential ones being:

Big Data and similar technologies should simply be prohibited, as they are contrary to the rights to privacy and data protection.

The regulation of privacy and data protection is outdated and only hampers innovation. Consequently, the laws should be changed or left unenforced.

Big Data is only a hype – so far, there is little evidence that Big Data technologies actually are effective. Thus, no changes to the legal regime are necessary.

Middle ground needs to be found to allow for new data technologies, while still respecting most of the privacy and data protection principles.

The current privacy and data protection regime should remain intact, but there should be a special and separate privacy and data protection regime for Big Data and similar technologies.

2.6. Conclusion and further reading

2.6.1 Conclusion

In conclusion, privacy is the concept that originally demarcated the private and the public domain. The king or ruler held sway over the public domain, the pater familias ruled as king over the household. Privacy has been protected in the legal domain throughout the ages, for example by granting a special legal status to the home of an individual, private correspondence and bodily integrity. Privacy is protected though civil law, such as tort and consumer law, through criminal law, and more recently, through constitutional law. How privacy is protected and what falls under its scope differs from jurisdiction to jurisdiction.

More recently, privacy has been incorporated in human rights instruments such as the Universal Declaration on Human Rights and the European Convention on Human Rights. The ECtHR has granted the right to privacy, provided under Article 8 ECHR, a very broad scope. The EU Charter of

Fundamental Rights contains a right to data protection, in addition to a right to privacy. Data protection is regulated in more detail in the EU by the General Data Protection Regulation. The GDPR provides detailed rules on how and when data controllers may legitimately process personal data of citizens. The US has a mostly scattered landscape when it concerns the right to privacy. There is considerable discussion among scholars about how privacy could and should be approached, such as seeing it as a personality right, a right that grants control over data, or even as a property right. The legal approach to privacy protection is challenged by new data technologies such as Big Data.

Below are some suggestions for further reading on specific topics.

Notes

Further reading

General literature

Aquinas, T. (1914-1942). The 'Summa theologica' of St Thomas Aquinas. City: Burns Oates and Washbourne.

Aries, P. & Duby, G. (1988). A History of Private Life: Revelations of the Medieval World, (Harvard: Belknap).

Austin, J. (1995). The Province of Jurisprudence Determined. Cambridge: Cambridge University Press.

Bentham, J. (1970). Of Laws in General. City: Athlone Press.

Derrida, J. (1989-1990). 'Force of Law: The Mystical Foundation of Authority', translated by Mary Quaintance, Cardozo Law Review 11, pages .

Fuller, L.L. (1969). The Morality of Law. City: Yale University Press.

Hart, H.L.A. (1994). The Concept of Law. City: Clarendon Press.

Hobbes, T (2006). Leviathan. Cambridge: Cambridge University Press.

Kantorowicz, E. (2016). The King's Two Bodies: A Study in Medieval Political Theology. Princeton: Princeton University Press 2016.

Koops et. al (2017). A Typology of Privacy. University of Pennsylvania Journal of International Law, 38(2).

Lessig, L. (1999). Code and Other Laws of Cyberspace. City: Basic Books.

Locke, J. (1988 [1689]). Two Treatises of Government. Cambridge: Cambridge University Press.

Montesquieu. (1989). The Spirit of the Laws. Cambridge: Cambridge University Press.

Rössler, B. (2005). The Value of Privacy. Cambridge: Polity Press.

Vasak, K. (1977). 'Human Rights: A Thirty-Year Struggle: the Sustained Efforts to give Force of law to the Universal Declaration of Human Rights', UNESCO Courier 30(11).

Privacy in the United States of America

Agre, P.E. and M. Rotenberg. (2001). Technology and Privacy: The New Landscape. City: MIT Press.

Allen, A.L. (2011). Unpopular Privacy: What Must we Hide? Oxford: Oxford University Press.

Benn, S.I. (1984). 'Privacy, Freedom, and Respect for Persons' in F. Schoeman (ed.), Philosophical Dimensions of Privacy: An Anthology. Cambrdige: Cambridge University Press.

Cohen, J.E. (2012). Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. New Haven: Yale University Press.

Cohen, J.L. (2002). Regulating Intimacy: A New Legal Paradigm. Princeton: Princeton University Press.

DeCew, J.W. (1997). In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. City: Cornell University Press.

Gavison, R. (1980). 'Privacy and the Limits of Law', Yale Law Journal 89, p. 455.

Gray, D. and D. Citron. (2013). 'The Right to Quantitative Privacy', Minnesota Law Review 101.

Hoofnagle, C.J. (2016). Federal Trade Commission Privacy Law and Policy. Cambridge: Cambridge University Press.

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. City: Stanford University Press.

Prosser, W.L. (1960). 'Privacy', Californian Law Review 48(383).

Regan, P.M. (1995). Legislating Privacy: Technology, Social Values, and Public Policy. City: University of North Carolina Press.

Solove, D.J. (2008). Understanding Privacy. City: Harvard University Press.

Warren, S.D. and L.D. Brandeis. (1890). 'The Right to Privacy', Harvard Law Review 4(5).

Westin, A.F. (1967). Privacy and Freedom. City:Atheneum.

Privacy under the Universal Declaration on Human Rights

Johnson, M.G. and J. Symonides. (1998). The Universal Declaration of Human Rights: A History of its Creation and Implementation. City: Unesco.

Robinson, N. (1958). The Universal Declaration of Human Rights: Its Origin, Significance, Application, and Interpretation. City: World Jewish Congress.

Schabas, W.A. (ed.). (2013). The Universal Declaration of Human Rights: the travaux préparatoires. (Cambridge: ambridge University Press.

Verdoodt, A. (1964). Naissance et signification de la Déclaration universelle des droits de l'homme. City: Warny.

Privacy under the European Convention on Human Rights

Arai-Takahashi, Y. The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR. City: Intersentia.

Dijk, P. van, F. van Hoof, A. van Rijk, and L. Zwaak (eds.). (2006). Theory and Practice of the European Convention on Human Rights. City: Intersentia.

Greer, S. (1997). The Exceptions to Articles 8 to 11 of the European Convention on Human Rights. City: Council of Europe.

Vande Lanotte, J. and Y. Haeck. (2004). Handboek EVRM. Dl.2 Artikelsgewijze commentaar, Vol. 1, Antwerpen. City: Intersentia.

Vande Lanotte, J. and Y. Haeck. (2004). Handboek EVRM. Dl.2 Artikelsgewijze commentaar, Vol. 2 (Intersentia 2004).

Ovey, C. and R.C.A. White. (2002). European Convention on Human Rights. Oxford: Oxford University Press.

Sloot, B. van der. (2015). 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of Big Data', Utrecht Journal of International and European Law 31(80).

Sloot, B. van der. (2017B). 'Where is the harm in a privacy violation? Calculating the damages afforded in privacy cases by the European Court of Human Rights', JIPITEC (4).

Data Protection, especially in the European Union

Burkert, H. (1983). Freedom of Information and Data Protection. City: Gesellschaft für Mathematik und Datenverarbeitung.

Bygrave, L.A. (2002). Data Protection Law: Approaching Its Rationale, Logic and Limits. City: Kluwer Law International.

Bygrave, L.A. (2014). Data Privacy Law: an International Perspective. Oxford: Oxford University Press.

Dammann, U., O. Mallmann, and S. Simitis (eds.). (1977). Data Protection Legislation: An International Documentation: Engl.-German: eine internationale Dokumentation: Die Gesetzgebung zum Datenschutz. City: Metzner.

Fuster, G.G. (2014). The Emergence of Personal Data Protection as a Fundamental Right of the EU. City: Springer.

Hondius, F.W. (1975). Emerging Data Protection in Europe. City: Elsevier.

Hijmans, H. (2016). The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU. University of Amsterdam Dissertation.

Sloot, B. van der. (2014). 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation', International Data Privacy Law 4.

Literature on debates and challenges

Privacy as control

Deci, E.L. and R.M. Ryan. (1985). 'The General Causality Orientations Scale: Self-determination in Personality', Journal of Research in Personality Volume(issue), pages.

Hornung, G. and C. Schnabel. (2009). 'Data Protection in Germany I: the Population Census Decision and the Right to Informational Self-determination', Computer Law & Security Review volume(issue), pages.

Rossnagel, A. and P. Richter. (2016). 'Big Data and Informational Self-Determination. Regulative approaches in Germany: The Case of Police and Intelligence Agencies' in van der Sloot, B., Broeders, D. and Schrijvers, E. (eds.), Exploring the boundaries of Big Data. Amsterdam: Amsterdam University Press.

Rouvroy, A. and Y. Poullet,. (2009).'The Right to Informational Self-determination and the Value of Self-development: Reassessing the Importance of Privacy for Democracy' in S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne, and S. Nouwt, Reinventing Data Protection? City: Springer.

Privacy as property

Epstein, R.A. (1977). 'Privacy, Property Rights, and Misrepresentations', Georgia Law Review 12(456), pages.

Hermalin, B.E. and M.L. Katz. (2006). 'Privacy, Property Rights and Efficiency: the Economics of Privacy as Secrecy', Quantitative Marketing and Economics volume(issue), pages.

Murphy, R.S. (1995). 'Property Rights in Personal Information: an Economic Defense of Privacy', The Georgetown Law Journal volume(issue), pages.

Posner, R.A. (1977). 'The Right of Privacy', Georgia Law Review volume(issue), pages.

Post, R.C. (1990). 'Rereading Warren and Brandeis: Privacy, Property, and Appropriation', The Case Western Reserve Law Review volume(issue), pages.

Purtova, N. (2012). Property Rights in Personal Data: a European Perspective. City: Kluwer Law International.

Privacy as personality right

Bloustein, E.J. (1964). 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', New York University Law Review 39(962), pages.

Eberle, E.J. (1997). 'Human Dignity, Privacy, and Personality in German and American Constitutional Law', Utah Law Review 963, pages.

Pound, R. (1915). 'Interests of Personality', Harvard Law Review 28(4), 1pages.

Schwartz, P.M. and K.-N. Peifer. (2010). 'Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?', California Law Review 98(1925), pages.

Strömholm, S. (1967). 'Right of Privacy and Rights of the Personality: a Comparative Survey', Nordic Conference on Privacy organized by the International Commission of Jurists, Stockholm.

Whitman, J.Q. (2004). 'The Two Western Cultures of Privacy: Dignity versus Liberty', Yale Law Journal 113(1151), pages.

Privacy and data protection

Fuster, G.G. and R. Gellert. (2012). 'The Fundamental Right of Data Protection in the European Union: in Search of an Uncharted Right', International Review of Law, Computers & Technology 26, pages.

Gellert, R. and S. Gutwirth. (2013). 'The Legal Construction of Privacy and Data Protection', Computer Law & Security Review 29, pages.

Hert, P. de. (1998).'Human Rights and Data Protection. European Case-Law 1995-1997', [Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak 1955-1997] in Jaarboek ICM 1997. City: Maklu.

Kokott, J. and C. Sobotta. (2013). 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', International Data Privacy Law 3, pages.

Lynskey, O. (2014). 'Deconstructing Data Protection: the "Added-value" of a right to data protection in the EU legal order', International and Comparative Law Quarterly 3, pages.

Balancing

Aleinikoff, T.A. (1987). 'Constitutional Law in the Age of Balancing', Yale Law Journal 97(5), pages.

Alexy, A. (2003). 'Constitutional Rights, Balancing, and Rationality', Ratio Juris 16, pages.

Cali, B. (2007). 'Balancing Human Rights? Methodological Problems with Weights, Scales and Proportions', Human Rights Quarterly 29(1), pages.

Greer, S. (2004). '"Balancing" and the European Court of Human Rights: a Contribution to the Habermas-Alexy Debate', The Cambridge Law Journal 63, pages.

Habermas, J. (1996). Between Facts and Norms. City: Polity.

Sloot, B. van der. (2016). 'The Practical and Theoretical Problems with "Balancing": Delfi, Coty and the Redundancy of the Human Rights Framework', Maastricht Journal of European and Comparative Law 3, pages.

Sloot, B. van der. (2017A). 'Ten Questions about Balancing', European Data Protection Law Review 2, pages.

Tsakyrakis, S. (2008). 'Proportionality: an Assault on Human Rights?', Jean Monnet Working Paper 09/08.

Big Data and privacy regulation

Ambrose, J. and M. Leta. (2015). 'Lessons from the Avalanche of Numbers: Big Data in Historical Context' I/S: A Journal of Law and Policy for the Information Society, http://ssrn.com/abstract=2486981.

Anderson, C. (2008). 'The End of Theory: The Data Deluge Makes the Scientific Method Obsolete', Wired Magazine 16 July, pages.

Andrejevic, M. (2014). 'The Big Data Divide', International Journal of Communication 8, pages.

Bollier, D. (2010). 'The Promise and Peril of Big Data', www.emc.com/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf.

Boyd, D. and K. Crawford. (2011). 'Six Provocations for Big Data', http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431.

Boyd, D. and K. Crawford. (2012). 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon', Information, Communication & Society 5, pages.

Crawford, C. and J. Schultz. (2014). 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms', Boston College Law Review 55, pages.

Davis, K. and D. Patterson. (2012). Ethics of Big Data: Balancing Risk and Innovation. City: O' Reilly Media.

Sloot, B. van der and S. van Schendel. (2016). 'International and Comparative Legal Study on Big Data', WRR-rapport, working paper 20, www.wrr.nl/publicaties/publicatie/article/international-and-comparative-legal-study-on-big-data/.

Legal documents

United States of America

Legal documents

US constitution and amendments https://www.usconstitution.net/const.html.

Federal Trade Commission Act https://www.law.cornell.edu/uscode/text/15/41.

The Children's Online Privacy Protection Act (COPPA) https://www.law.cornell.edu/uscode/text/15/6501.

The Health Insurance Portability and Accountability Act (HIPAA) https://www.law.cornell.edu/uscode/text/42/1301b.

The Fair Credit Reporting Act https://www.law.cornell.edu/uscode/text/15/1681.

The Electronic Communications Privacy Act https://www.law.cornell.edu/uscode/text/18/2510.

Constitution of Alaska https://www.commerce.alaska.gov/web/Portals/4/pub/AK%20CONSTITUTION-Citizens%27%20Guide.pdf.

Constitution of California http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I.

Constitution of Florida http://dos.myflorida.com/media/693801/florida-constitution.pdf.

Constitution of Montana https://courts.mt.gov/portals/113/library/docs/72constit.pdf.

California Electronic Communications Privacy Act
https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178.

Supreme Court cases

Supreme Court, Olmstead v. United States, 277 U.S. 438 1928.

Supreme Court, Griswold v. Connecticut 381 U.S. 479 1965.

Supreme Court, Katz v. United States 389 U.S. 347 1967.

Supreme Court, Roe v. Wade 410 U.S. 113 1973.

Supreme Court, Riley v. California 13-132, 573 U.S. 2014.

United Nations

Universal Declaration on Human Rights www.un.org/en/universal-declaration-human-rights/.

International Covenant on Civil and Political Rights
www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

Council of Europe

Legal documents

Council of Europe, Original European Convention on Human Rights
www.echr.coe.int/library/annexes/CEDH1950ENG.pdf.

Council of Europe, Current European Convention on Human Rights
www.echr.coe.int/Documents/Convention_ENG.pdf

Council of Europe, Committee of Ministers, Resolution (73) 22 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the private sector. (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies).

Council of Europe, Committee of Ministers, Resolution (74) 29 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the public sector. (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies).

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28 January 1981.
http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm.

Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981 https://rm.coe.int/16800ca434.

Council of Europe, Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms Paris, 20.III.1952.

Council of Europe, Protocol No. 8 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Vienna, 1985.

Council of Europe, Protocol No. 9 to the Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 6 November 1990. This Protocol has been repealed as from the date of entry into force of Protocol No. 11 (ETS No. 155) on 1 November 1998.

Council of Europe, Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, restructuring the control machinery established thereby. Strasbourg, 11 June 1994. Since its entry into force on 1 November 1998, this Protocol forms an integral part of the Convention (ETS No. 5).

ECtHR jurisprudence

ECtHR, Klass and others v. Germany, application no. 5029/71, 6 September 1978.

ECtHR, B. v. the United Kingdom, Application no. 9840/82, 8 July 1987.

ECtHR, P.G. and J.H. v. the United Kingdom, application no. 44787/98, 25 September 2001.

ECtHR, S. and Marper v. the United Kingdom, application no. 30562/04 30566/04, 04 December 2008.

ECtHR, Delfi v. Estonia (Grand Chamber), application no. 64569/09, 16 June 2015.

ECtHR, Roman Zakharov v. Russia, application no. 47143/06, 04 December 2015.

ECtHR, Szabó and Vissy v. Hungary, application no. 37138/14, 12 January 2016.

European Union

Legal texts

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Charter of Fundamental Rights of the European Union (2000/C 364/01). www.europarl.europa.eu/charter/pdf/text_en.pdf.

2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, also known as the e-Privacy Directive), Official Journal L 201, 31/07/2002 P. 0037–0047.

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

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30 December 2008.

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

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

ECJ case law

European Court of Justice, Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, 8 April 2014.

European Court of Justice, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, case C-131/12, 13 May 2014.

European Court of Justice, Maximillian Schrems v. Data Protection Commissioner, joined party: Digital Rights Ireland Ltd, Case C-362/14, 6 October 2015.

European Court of Justice, Tele2 Sverige AB (C-203/15) v. Post-och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v. Tom Watson, Peter Brice, Geoffrey Lewis, interveners: Open Rights Group, Privacy International, The Law Society of England and Wales, Joined Cases C-203/15 and C-698/15, 21 December 2016.

Organization for Economic Co-operation and Development

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data from 1980 www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Regional human rights documents

American Convention on Human Rights adopted in 1969 www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm.

African Charter on Human and Peoples' Rights from 1981 www.humanrights.se/wp-content/uploads/2012/01/African-Charter-on-Human-and-Peoples-Rights.pdf.

Association of Southeast Asian Nations (ASEAN) Human Rights Declaration from 2012 http?aichr.org/?dl_name=ASEAN-Human-Rights-Declaration.pdf.

European constitutions

Dutch constitution https://www.government.nl/documents/regulations/2012/10/18/the-constitution-of-the-kingdom-of-the-netherlands-2008.

German Constitution https://www.btg-bestellservice.de/pdf/80201000.pdf.

Italian Constitution
https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf.

Spanish Constitution
www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm/const_espa_texto_ingles_0.pdf.