THE RIGHT TO PRIVACY AS A HUMAN RIGHT AND EVERYDAY TECHNOLOGIES

Legal aspects of privacy law and data protection

Katrin Nyman Metcalf

TABLE OF CONTENTS

TABLE OF CONTENTS 82

INTRODUCTION 83

HOW PRIVACY LAW DEVELOPED: HISTORICAL BACKGROUND 84

MAIN LEGAL PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA 85

THE RIGHT TO PRIVACY AS A HUMAN RIGHT 86

PRIVACY LAW AND PERSONAL DATA PROTECTION IN EUROPEAN AND ESTONIAN LAW 90

EUROPEAN UNION LAW IN THE FIELD OF DATA PROTECTION 90

LEGAL SYSTEM OF ESTONIAN DATA PROTECTION 92

THE ESTONIAN CONSTITUTION 92

PERSONAL DATA PROTECTION ACT AND OTHER LEGAL ACTS 93

SUPERVISION 94

FINAL NOTE: CHALLENGES FOR DATA PROTECTION LAW 96

INTRODUCTION

Total privacy is impossible in a society where people together. Modern information and communication technologies (ICT) have facilitated new ways of communicating, distributing and gathering information, socialising with friends and meeting new people, giving advice, governing and much more. We can now communicate directly with virtually the entire world in ways that were unthinkable only a few decades ago. Along with the many advantages, the new modes of communication also create risks. If the whole world becomes a village in which everybody knows one another, what will become of privacy? People's views must be considered, but we also have to understand the legal context that frames the attitudes.

Legally, data protection is part of privacy law, which is protected as a human right both in national constitutions and international conventions.[1] This means that the principles of data protection existed before data protection was discussed as such or specific laws on that issue were adopted. The connection continues to be important today. Even countries that lack a separate legislative act on data protection honour the right to data protection to a certain extent as nearly all countries on earth have acceded to at least some human rights conventions. Estonia has a number of provisions in its Constitution and other legislation that protect privacy and data. In addition, there is independent data protection oversight, which is exercised by the Data Protection Inspectorate.

Data protection as a separate topic in legal science discourse and legislative practice arose in the 1970s and 1980s, in the era in which computerised automatic data processing became the norm. With technological progress, data have become very valuable and important. Great volumes of data can be used to provide different services; this was not possible before automated processing. Data exchange and cross-use are important for public and private services based on various data. Still, the nature of data protection should be related to the content of the data and not to their form. It is not important, in principle or legally speaking, whether the data are preserved and processed electronically or in some other manner. In practice, it could mean key differences that the legal system must take into consideration to ensure that the rules are suitable in different situations. With regard to data protection, it must be decided how, if at all, data can be protected to the same extent in the virtual as in the "real" world. It is not unusual that attempts to create a safe online society result in even more restrictions than in an offline environment. Technologies may also offer new opportunities for more effectively guaranteeing data protection. Thanks to modern technologies, data processing has also become more secure, instead of only creating new risks. For example, operations leave a "footprint" in a database, meaning that if someone views data, logs can be checked to verify when and by whom the access occurred. This significantly reduces the risk of abuse of data by officials or negligence and helps to increase people's trust in electronic databases.

[1] Section 1 of the Personal Data Protection Act stipulates that the purpose of the Act is to safeguard the fundamental rights and freedoms of individuals, above all the inviolability of private life.

A number of scandals covered in the media – concerning wiretaps or e-mail snooping – has led to debate about the meaning and importance of privacy. Even so, the way people behave continues to result in an abundance of data more or less publicly available about them. This is done through use of Facebook or by merely carrying a mobile telephone with them, which allows their position to be known. From the standpoint of data protection, one must consider what data are of a kind where general availability should be restricted. Certain data – no matter what form they are in – may be generally visible or otherwise available. As people's awareness of how data can be protected is often not all that high, the legal system should offer support to support activities aimed at increasing awareness.

HOW PRIVACY LAW DEVELOPED: HISTORICAL BACKGROUND

Data protection is not in itself related to modern technology yet its importance has certainly increased due to technology. The world's first law on data protection was adopted in Hessen, Germany, in 1970. Sweden was the first country to adopt a law on data protection, in 1973, and it was followed by legislation in a number of other countries.[2] The first major international document that expressed the main principles of data protection, such as expedience and proportionality, was the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data from 1980.[3] In December 1983, the Constitutional Court of Germany adopted a decision under which certain aspects of a census were considered to run counter to fundamental liberties due to the inviolability of personal privacy.[4] All of this happened at a time when more computer-based data processing began to be used. Technology showed the importance of data protection, as it was possible to process a very large amount of data to obtain some useful information from them. Technology can be used to glean meaning from a large set of detailed data – various data can be collated so that insignificant data take on importance, and data can be gathered and disseminated worldwide. Technology is undoubtedly responsible for creating a new environment in which data protection must be implemented. [5]

The context of data protection in the OECD guidelines and European Union legal acts is the processing of data and, in particular, the movement of data between countries. In the 1970s and 1980s, such data movement was a time-consuming and labour-intensive process, and various rules could be applied to the process. The technical possibilities of automatic data exchange were a key reason for establishing rules for the exchange of data, as it was no longer possible to study in detail how data in each incident should be handed over to other countries and/or authorities.

---

[2] Fraunhofer Fokus (P. Hoepner, L. Strick, M. Löhe) *Historical Analysis on European Data Protection Legislation.* Report March 2012, pp. 11-12. www.fokus.fraunhofer.de

[3] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm The document was amended in 2013.

[4] Fraunhofer Fokus Report 2012, p. 12.

[5] G. Gonzales Fuster, S. Gutwirth & P. de Hert (2010) "From Unsolicited Communications to Unsolicited Adjustments": G. Gutwirth,Y. Poullet & P. de Hert (ed.) *Data Protection in a Profiled World*, Springer, Dordrecht/London (105-117): pp. 107-109.

Due to the rapid progress of ICT in the last 20 years, a new situation has now arisen whereby private corporations possess a large amount of data on people – data they have obtained from the individuals themselves – either directly, though the people putting the data online (e.g. Facebook) or people using an Internet service that allows various things to be found out about them (Google). A number of companies, including major international companies such as Facebook and Google, have ethical rules and different structures for implementing the rules. But these are rules the companies have themselves seen fit to establish and are mainly based on the goodwill of the respective companies. In addition, national legislation is in force regardless of the fact that the companies are multinationals and it may be difficult to establish a direct link to a given jurisdiction in a specific case. However, laws could, in fact, prove difficult to apply precisely due to reasons related to jurisdiction.

MAIN LEGAL PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA

The laws on data protection and the system for implementing the laws have changed little since the advent of the field. The reason for protecting data is that the content of the data has an impact on the private lives of individuals, which should be inviolable and decided over solely by the people themselves. The specific rules for data protection include, for instance, the right to gain access and correct information about oneself. It is important for the person to know what these data are and to be able to check that they are correct. Oversight is an important part of data protection, as it cannot be decreed for each situation what data can be shared and in what manner – the situations vary too widely. It is important that there is an independent authority responsible for data protection oversight and that the oversight includes the classification of various data. As regards institutions, it is important that there are competent individuals responsible for the data. It continues to happen that the IT departments of authorities are responsible for all issues related to electronic data, including matters that are more related to content than form of the data and with which persons with a different competence should deal.

The consent of the individual is an important aspect of data protection. Consent is often required for gathering and processing data, although there are also various situations where countries (usually not private businesses) are permitted to gather certain data even without consent. The consent must be informed. That means the individual has enough information to understand what he or she is consenting to and that he or she is doing so voluntarily. The person may withdraw his or her consent at any time.

The data protected are personal data containing all kinds of information on identified or identifiable natural persons, considering that a person is identifiable if he or she can directly or indirectly be identified, particularly by a personal identification code or one or more of his

or her physical, physiological, mental, economic, cultural or social identity traits.[6] Data may vary in terms of sensitivity but all data on identified persons are personal data as far as the law is concerned, and they are to be processed in accordance with the established procedures. The goal of data protection legislation is, above all, to ensure a procedure for data processing, not hinder it. Data are important for society, but they are to be dealt with so that their correctness is ensured and the use for non-designated or harmful purposes is prevented.

In the majority of countries, current legislation specifies separately what is meant by sensitive personal data. EU Directive 95/46/EC makes separate mention of personal data that reveal racial or ethnic origin, political views, religious or philosophical convictions, membership of trade unions, and a person's state of health or sex life.[7] Each country establishes a precise definition for sensitive personal data, both in legislation and through judicial practice, and as a result cultural and historical differences can be seen from one country to another.[8]

THE RIGHT TO PRIVACY AS A HUMAN RIGHT

The UN Universal Declaration on Human Rights[9] from 1948 and the European Convention on Human Rights[10] from 1950 include the concept of the right to privacy or the inviolability of private life, which continues to be the basis for data protection. Regional human rights conventions outside Europe also enshrine similar rights. The first key human rights document

[6] Article 2, Directive 95/46/EC. Several data protection acts, above all in the EU but elsewhere as well, use very similar terminology.
[7] Article 8, Directive 95/46/EC.
[8] The relevant provision from the Estonian Personal Data Protection Act:
§ 4. Personal data
(1) Personal data are information relating to an identified natural person or a natural person identifiable by reference to the person's physical, mental, physiological, economic, cultural or social characteristics, relations and associations.
(2) The following are private personal data:
1) data revealing details of family life;
2) data revealing an application for the provision of social assistance or social services;
3) data revealing mental or physical suffering endured by a person;
4) data collected on a person during the process of taxation, except data concerning tax arrears.
(3) The following are sensitive personal data:
1) data revealing political opinions or religious or philosophical beliefs, except data relating to being a member of a legal person in private law registered pursuant to the procedure provided by law;
2) data revealing ethnic or racial origin;
3) data relating to the state of health or disability;
4) data relating to genetic information;
5) data relating to sexual life;
6) data concerning membership in trade unions;
7) information collected in criminal proceedings or in other proceedings to ascertain an offence before a public court session or before a judgment is made in a matter concerning an offence, or if this is necessary in order to protect public morality or the family and private life of persons, or where the interests of a minor, a victim, a witness or justice so require.
[9] http://vm.ee/et/uro-inimoiguste-ulddeklaratsioon
[10] https://www.riigiteataja.ee/akt/78154

that directly refers to data protection is the EU Charter of Fundamental Rights, which was promulgated in 2000 and was made legally binding and became a part of the EU treaties under the Lisbon Treaty, which entered into force in 2009. The Charter refers to data protection in Article 8; general privacy protection is set forth in Article 7. Before the Charter, data protection was only supported by way of Articles dealing with privacy. Article 8 of the EU Charter of Fundamental Rights gives everyone the right to access and have rectified information collected concerning him or herself.[11]

Unlike the EU Charter of Fundamental Rights, data protection is not separately regulated in conventions or similar documents on a global level. However, the right to privacy does exist and, hence, certain data protection. A number of countries lack data protection laws, and although such countries can implement certain data protection under privacy rules via the courts or other institutions, it is evident that such protection is more general and less effective than in places that do have data protection laws. In the case of data protection, there are no international (global) standards as there are in the case of freedom of speech. The broader standards are limited to what can be classed as privacy. Although the EU requires there to be an independent authority with responsibility for data protection, and such authorities exist elsewhere in the world, it cannot be said that this requirement stems from universal principles of law. Differences between even relatively similar legal systems can be seen between the EU and the US, for instance. The United States lacks a general data protection act; instead, rules are established ad hoc for the various fields. For two different reasons, data protection is less effective in the US than it is in the EU. On the one hand, freedom of expression is even more strictly protected in the US than it is in Europe. Because of this, restrictions on use of information are rare, even if privacy may be infringed on to a certain extent by the contents of the data. The other difference stems from a completely different reason: as there is no general law on data protection and no independent oversight, it is simpler to restrict privacy in the interests of national security.

The latter difference between the EU and US can be seen in the differences of opinion as pertains to the exchange of PNR data in the aviation sector – in this case, the kind of data exchange[12] the US requested in return for airspace access rights went against the EU's rules on data protection. The topic has been discussed since early 2000. In 2007, an agreement was reached, in 2011 it was amended, and the topic remains constantly under discussion. As modern technology is essentially global, we must be aware that although universal rights exist there are variations in terms of the details of their implementation. The particularity of public international law is that there is no global legislature, and the only way to reach international rules is through negotiations.
The fundamental legitimacy of data protection derives from the right to the inviolability of private life. Privacy or the inviolability of private life is enshrined in major international conventions such as the UN Universal Declaration of Human Rights[13] (Article 12)[14] and the

[11] K. Nyman-Metcalf (2014:2) "The Future of Universality of Rights": T. Kerikmäe (ed.) *Protecting Human Rights in the EU*, Springer, Heidelberg (21-35): pp. 28-30.
[12] PNR *Passenger Name Record Data*
[13] http://vm.ee/et/uro-inimoiguste-ulddeklaratsioon

European Convention on Human Rights and Fundamental Freedoms[15] (Article 8)[16]. The right to privacy includes various things such as protection of the secrecy of mail, telephone calls and other communications, inviolability of the home, protection against libel and slander; and data protection. Courts determine case by case what the right precisely encompasses. The links between data protection and privacy indicate that data protection by its very nature is linked to private life and the right to decide on whom the data related to private life are shared with and how they are shared. To a certain extent, this connection limits data protection, as data that are not related to private life or data that can be distributed without impacting the inviolability of private life are not protected unless a specific law has been passed to grant protection to them. For example, these might include data related to business or other professional activity or data that are easily available and are therefore not considered of a type that should have much of an effect on people's private lives. The same connection between privacy and data protection also means that in countries lacking a data protection law or in situations where such a law is not in effect for various reasons, there may still be a certain level of data protection based on the right to privacy.

Like most human rights, the right to privacy is not absolute; it can be restricted in certain situations and due to other rights. Courts often deal with the relationship between freedom of expression and privacy. [17] The courts must on the one hand weigh up the reasons for publishing certain information and, on the other hand, the potential impact on an individual of such public disclosure. A proportionate solution must be found, in which public interests (including free debate and the opportunity to obtain all manner of information) as well as the interests of the individual are taken into consideration. In democracies that respect freedom of expression, there are few restrictions on what can be published in the media or otherwise. In particular, people who occupy some public position must tolerate the prospect of negative information being spread regarding them; examples include cartoons, satire, criticism, etc.

The goal of human rights is to protect major fundamental freedoms and rights and to create a system that ensures that individuals cannot infringe upon the rights of others. In the field of privacy, the European Court of Human Rights has set judicial precedents. In general, judicial practice mandates (with regard to any restriction of rights) that any restriction of human rights must be stipulated in law, proportionate and necessary in a democratic society. Laws that are not proportionate and necessary may infringe on human rights, and situations may occur whereby the necessary laws do not exist or are not implemented properly. Both problems can crop up in relation to modern media and social networks: inappropriate laws (or other rules) or a deficient legal framework. As with new technologies, it is often hard to

---

[14] 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.*

[15] https://www.riigiteataja.ee/akt/78154

[16] Article 8 *(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

[17] Supreme Court, legal information department, Eve Rohtmets „Ajakirjandusvabaduse ja eraelu puutumatuse tasakaal Euroopa Inimõiguste Kohtu praktikas. Kohtupraktika analüüs", Tartu March 2014, www.riigikohus.ee

see if and how a certain activity can be impacted with laws and other rules (whether due to matters of jurisdiction, to the fact that it is difficult to implement existing legislation for new and complicated technologies, or for other reasons). There are many situations in which people feel (and this is also expressed in public discourse) that the situation should be regulated, that something should be prohibited, that it should be possible to halt a certain activity and so on – although the legal system actually does not have the necessary instruments to accomplish this. In democracies that respect human rights and fundamental freedoms, it is still important to permit everything that is not specifically prohibited by legislation, not the opposite (activities are illegal if not expressly allowed by law).

PRIVACY LAW AND PERSONAL DATA PROTECTION IN EUROPEAN AND ESTONIAN LAW

EUROPEAN UNION LAW IN THE FIELD OF DATA PROTECTION

EU data protection rules can be found in Directive 95/46/EC of the European Parliament and of the Council, 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[18] The purpose of the Directive is to protect the rights and freedoms of natural persons with regard to processing personal data and to ensure that they are implemented in unified fashion in all member states by establishing principles for data protection.

The Directive is currently under review[19] for the purpose of making the rules more appropriate for modern technologies and to ensure that there are no major differences between countries as is currently the case. For the latter reason, it is planned to adopt a Regulation instead of the Directive. The Regulation would be directly applicable in every member state without having to be transposed into national legislation. This ensures greater uniformity between member states.

In addition to the main data protection Directive, there are a number of more specific legal acts that encompass data protection in specific situations. This includes Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [20] and Directive 2002/58/EC, which deals with the processing of personal data and protection of the inviolability of private life in the electronic communication sector.[21]

The EU also has a Directive – 96/9/EC – on databases[22], but it only deals with databases from the perspective of intellectual property law and does not encompass data protection. Another Directive that deals with data is 2003/98/EC on the re-use of public sector information.[23] This Directive has an indirect impact on the situation with data protection, as it

[18] 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 (OJ L 281, 23/11/1995, p. 31).
[19] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
[20] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17/07/2001, p. 01).
[21] 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) (OJ L 201, 31/07/2002, p. 37).
[22] Directive No. 96/9/EC of the European Parliament and of the Council, of 11 March 1996 on the legal protection of databases (OJ L 77/20, 27/03/1996, p. 459).
[23] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31/12/2003, p. 90).

sets forth that information in the public sector may be used for commercial purposes, thereby creating added value from the data. The Directive refers to the data protection Directive and does not establish new rules; rather, it supposes that the data are protected. In addition, there is also Council framework decision 2008/977/SK on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, and other non-binding acts, which simplify cooperation between member states.

In EU judicial practice over the years, there have been a number of cases with regard to data protection, through which more definite frameworks for interpretation of the Directives have been established. Through these cases, it has clearly been seen that different member states have different understandings – and this is one reason for EU data protection reform. Court decision C-131/12 in 2014 is especially interesting, as it deals with the right to be forgotten. In short, the court decided that Google must remove from its search results certain information that could be negative to individuals if there was no reason in the public interest for the information to be available. Although such a rule could seem to be in conformity with the principles of data protection and privacy, various risks can be seen with a more in-depth analysis: For instance, a private corporation – Google – could have a way of "deleting" history. To keep such actions from being too widespread, a strict system has been created to regulate for which situations an application can be made regarding the removal of information. An excessively broad deletion of data would pose a threat to the freedom of expression and the right – a general human right – of seeking and acquiring information, but overly strict requirements might result in the real meaning being lost. In addition, the system is primarily in force in the EU. To date, similar decisions elsewhere in the world have not been made and, through the global nature of the Internet, the same information could be available elsewhere, which could mean that in fact the EU court has merely engendered a false sense of security with regard to the possibility of deleting an inconvenient history; this may even lead to people becoming less circumspect with regard to sharing personal data.

Data protection laws and the EU Directive elucidate the terms that are used in legal acts. The data protected are personal data containing all kinds of information on identified or identifiable natural persons, considering that the person is one who can directly or indirectly be identified, particularly by a personal identification code or one or more of his or her physical, physiological, mental, economic, cultural or social identity traits.[24] Data may vary in terms of sensitivity, but all data on identified persons are personal data as far as the law is concerned and they are to be processed in accordance with the established procedures.

In addition to data protection rules, there are other legal areas that impact on the data-related aspects, especially in connection with modern ICT such as social networking. Consumer protection law is one of these. As parties to transactions in e-commerce and e-service are not present in the same place and at the same time – there is no face-to-face contact – it is particularly important that transactions are understandable and that consumers are aware of what they are consenting to. And as all sorts of additional services are possible for various e-services and these are only partially related to the original service, it must be ensured that the consent is informed consent. This can be done by requiring that

[24] Article 2, Directive 95/46/EC. Many data protection acts, above all in the EU but elsewhere as well, use very similar terminology.

terms of use be available and that people can confirm on the website that they have read the terms. For instance, the EU bans automatically selected service enhancements. Rather, actions are required – true, this usually involves only ticking a checkbox on a website. Actually, it is impossible for such measures to guarantee that individuals are indeed aware and that their consent is given voluntarily and deliberately. Yet, it is also hard to imagine how the legal system could accomplish this in any other way: ultimately, every individual is responsible and a rise in awareness can be achieved through education, campaigns, the media and other means.

LEGAL SYSTEM OF ESTONIAN DATA PROTECTION

The Estonian Constitution

The Constitution has a number of sections on various aspects of privacy. Article 26 sets forth the inviolability of family and private life and Article 33, the inviolability of the home. Article 42 forbids government authorities, local governments and officials thereof to gather and store data on the convictions of Estonian citizens against their free will. The secrecy of communication channels is set forth in Article 43. Access to information and data protection are guaranteed by Article 44.

§ 44. *Everyone has the right to freely obtain information disseminated for public use.*
All state agencies, local governments, and their officials have a duty to provide information about their activities, pursuant to procedures provided by law, to an Estonian citizen at his or her request, except information the disclosure of which is prohibited by law, and information intended exclusively for internal use.
An Estonian citizen has the right to access information about himself or herself held in state agencies and local governments and in state and local government archives, pursuant to procedure provided by law. This right may be restricted pursuant to law to protect the rights and freedoms of others or the confidentiality of a child's filiation, and in the interests of combating a criminal offence, apprehending a criminal offender, or ascertaining the truth in a criminal procedure.
Citizens of foreign states and stateless persons who are in Estonia have the rights specified in paragraphs two and three of this section equally with Estonian citizens, unless otherwise provided by law.

The right to verify information about oneself – the right to "informational self-determination," so to speak – is the foundation of the principles of protection of personal data.

Personal data protection act and other legal acts

The primary law on data protection in Estonia is the Personal Data Protection Act, which was adopted on 15 February 2007.[25] The Act sets out the conditions and procedure for processing personal data, the state supervision procedure for processing personal data and the responsibility for violation of the requirements.

The Act is based on the EU Directive and is in conformity to it. As mentioned, one of the purposes behind the EU reform is that it should create, in place of a Directive, a Regulation that would be directly applicable in member states. At the same time, even after such a reform, a number of principles would remain in force in both EU and Estonian law.

The first section of the Personal Data Protection Act refers to the inviolability of private life and the fundamental rights and freedoms of the individual in general.

The Act sets forth principles for processing personal data that a responsible and authorised processor of personal data must follow. It is also important that such a responsible person (chief processor) be appointed (Article 7). In processing data, the processors of personal data must follow the main principles of data protection: legality, expedience, minimality and the principle of restricting use, as well as data quality, security and individual participation. The last of these means that a data subject must be notified regarding data on him or her, and the subject must be given access to data on him or her and that he or she has the right to request the correction of inaccurate or misleading data. This right is implemented in greater detail through other provisions of this Act. The principles of expedience and limited use stipulate that personal data may only be collected for defined and legitimate purposes, and personal data may be used solely for other purposes with the consent of the data subject or with the consent of a competent authority.

While, in general, the processing of personal details is permitted with the consent of the data subject, there are a number of situations in which data can also be processed in the absence of consent. These situations are specified in legislation (Article 14). For instance, in cases set forth in legislation or for performing functions arising from legislation, for performing a contract entered into with a person, in the case of overriding public interest, etc.

Article 5 of the Act sets forth the nature of the processing of personal data. The text comes from the EU Directive and states that processing is "any operation or set of operations which is performed upon personal data, such as collection, recording, organisation, storage, alteration, grant of access, consultation, retrieval, use, transmission, cross-usage, combination, blocking, erasure or destruction, or several of the aforementioned operations regardless of the manner in which they are performed or the means used". In certain situations, such as the processing of data for personal purposes, the law is not applied. Otherwise, the definition of processing would be so broad that it covers any use of data.

[25] RT 2007, 24, 127.

The Personal Data Protection Act provides very general guidelines for the protection of personal data (Articles 25 and 26). Specifically, the evaluation of the security class and determining and implementing appropriate security measures is agreed with different Government of the Republic regulations.[26] In larger companies that deal with data security, internationally recognised security standards[27] and methodologies are applied – either voluntarily or due to legal acts and requirements in the field. Determining the security level of data is important as this determines on how the data will be protected in further instances. This means that the instance deciding on various data must be competent to do so.

The responsibility of communications undertakings for data also derives from Chapter 10 of the Electronic Communications Act[28] on the security and protection of data. Communications undertakings have the obligation to ensure data protection and to process data so that the principles of data protection are not violated. In the case of violations related to personal data, communications undertakings are obliged to notify the Data Protection Inspectorate as soon as possible (Article 102). In part, the purpose of the Electronic Communications Act is to ensure that communication undertakings – who deal with data, after all – ensure the principles of data protection in their activities. The Electronic Communications Act also includes specific rules with regard to various data, such as data on the location of customers (Article 105). The main rule is that such data must be made anonymous or that there must be consent from the data subject – the client – for processing the data.

In addition, data protection is mentioned in various regulations on specific data processing systems.

Supervision

An important part of the EU data protection system is that every country must have a data protection inspectorate or other independent authority with the competence to ensure supervision over the data protection situation in the country, including at government authorities. The inspectorate should be empowered to receive complaints and initiate investigations. In addition, the inspectorate is usually the body that hands out licences to process data. Through these means, it investigates the planned systems. In a number of countries outside the EU as well, there are data protection authorities, and in a number of cases they were inspired by EU rules. It is possible that other authorities, such as an ombudsman, also deal with data protection. It is important that the supervision is effective and that it is clear where problems should be addressed. As the purpose for establishing the authority is to advise and teach about how to deal with data, it is also important that the activities of the authority are largely public and the decisions and recommendations easily available. Good practices are established in this manner. Even in the case of problems, it

[26] For example, the Government of the Republic regulation on the system of security measures for information (RT 1, 2007, 71, 440) and information security management (RT I, 19.03.2012, 4), and the Government regulation, established on the basis of the Emergency Act, on information systems for vital services and security measures for information resources related (RT I, 20.03.2013,7).
[27] For example, the EVS-IEC/ISO 27001, etc. standard families.
[28] RT I 2004, 87, 593.

often happens that the inspectorate does not decide on consequences but merely points out problems and advises on what should be done differently.

The statute of the Estonian Data Protection Inspectorate sets forth the main functions:

§ 9. Main functions of inspectorate
The main functions of the inspectorate shall be:
1) exercise state supervision over the compliance with the legislation regulating the area of activity of the inspectorate and, if necessary, to apply state coercion.
2) participation in the development of legislation concerning its area of activity and making proposals for the amendment and supplementation thereof.
3) participation in the development of the policy, strategy and development plans related to the area of activity thereof;
4) preparation and implementation of the projects related to its area of activity, including participation in the preparation and implementation of international projects;
5) participation in the work of international working groups and organisations concerning its area of activity.

The Data Protection Inspectorate has both a supervisory and a general department. One of the important roles of the Data Protection authorities is public relations and preventive work. The general department of the Data Protection Inspectorate deals with information advisement, cooperation and other similar work.[29] Decisions, guidelines and general information on the protection of privacy and public information are available online. There are many guidelines on various specific topics,[30] such as information security and the protection of personal data in small enterprises or personal mobile equipment in the working environment. Together, the guidelines and decisions help create a more effective data protection system, one that should also be understandable to laymen.

The website of the Data Protection Inspectorate has information on what action to take in the event of a complaint on data processing.[31] It provides various examples of complaints along with explanations, sample forms and other necessary information. The text is clear and the samples help people convey important information. The activities of the Inspectorate are aimed at ending violations, as described on the website. In certain cases, it may still be necessary to go to court. Signs of misuse can also be reported if this does not have a direct impact on an individual. Although the necessary information and procedures are in place and are clearly described, many people lack knowledge about what should be done for data protection when they have concerns that the processing of personal data may be problematic.[32] The inspectorate could try harder to notify the media and utilise various channels but, besides this, it is difficult to see what more it could do if people do not themselves look for information that is, after all, available.

[29] http://www.aki.ee
[30] http://www.aki.ee/et/eraelu-kaitse/juhised
[31] http://www.aki.ee/et/inspektsioon/poordu-inspektsiooni-poole
[32] This was shown by a public opinion poll, which is part of this study.

FINAL NOTE: CHALLENGES FOR DATA PROTECTION LAW

Human history has seen constant changes in society, technology, everyday life and people's convictions. Still, the changes in recent decades have taken place faster than ever before and everyday life has seen greater transformation than in the past. This poses a challenge for implementing rights and legislation. In complicated times when people do not understand how to act in the context of constant new activities, technologies and contacts, they expect support from outside – such as legislation and the implementation of legislation. This tendency can be seen in the context of privacy and data protection, where new communication technologies and methods have led to new challenges and threats. However, existing legislation has a hard time coping with such challenges and threats and for a number of reasons it is difficult to pass new, more suitable laws. Instead, people's own responsibility is greater at times in which they tend to expect greater support.

In Estonia, as in the majority of EU member states, private life is protected by law, and rules and supervision systems have been established for data protection. In spite of this, it happens that data are abused or they fall into the wrong hands. Although certain reforms are undoubtedly necessary to address modern technologies more effectively, it cannot be said that there are major problems with data protection rules. It is hard to implement any rules in such a rapidly changing and international society with its modern social network, especially when people are constantly sharing more information about themselves with an ever wider audience.

A phenomenon that has been seen throughout history is that there are differences in views, and beliefs and skills also vary. Changes in this field have also been faster in recent times. With regard to data protection and privacy, this means that younger people who grew up using interactive communication technologies, which make personal information easily and widely available, see privacy differently than their elders. Legislation and its implementation have been founded on older convictions. One of the roles of the legal system is to influence people's behaviour and their understanding of society and its rules, but such an influence must have some virtuous, purposeful goal. We should ask ourselves: if people do not see and sense danger, should they still be protected?

In the context of a person's own responsibility, it is legally important as to whether consent for some activity or act has been given and whether the consent was voluntary and deliberate. There are also some situations whereby some activities are not allowed, even with consent. An activity as such may be prohibited as generally harmful or in contravention with professional ethics, or the use of data could restrict the privacy of third parties. More frequent are situations in which consent may be granted formally but where it was not voluntary or informed. The reason for such a case may be that the person did not understand what he or she gave consent for – perhaps the situation was so complex, the information deficient or the subjects lacked the ability to adequately understand the situation. The reason

may however also be that although the person understood and did not want to give consent, he or she actually had no choice, as otherwise – had he or she not consented to a certain activity, he would have forgone something else that was important. For instance, there are services that require a Facebook or Twitter account, and thereby giving up such networks would also mean giving up other services (such as the opportunity to read and comment on certain electronic periodicals, etc.). Many such situations arise in connection with modern information technology: some where people do not understand the situation because the technology is so complex, and others where technologies have become so important that failing to adopt them makes life in modern society difficult.

People's own responsibility is about more than just being aware of various terms of use and giving consent for solely collecting or processing the data that they are actually ready to allow; they also have the responsibility to act so that they minimise the risks that data will end up in a situation in which they cannot be protected. Often a non-electronic explanation is found instead – i.e. that the problem is not in technology but how it is used – perhaps the explanation is as simple as someone leaving the door open to a room containing a computer with sensitive data, or lost a memory stick containing data.[33]

Technology may be more efficacious in protecting data, for example by providing an alert if data are misused. In any case, the data protection aspect must be part of an evaluation of information systems – both how the system can help to ensure better data protection and by examining what potential risks crop up and how to combat them effectively yet proportionally.[34] Recently, there has been much reference made to the principle of privacy by design. It is also found in the new EU Data Protection Regulation. The main aim behind this principle is for data protection to be built into IT system design and architecture as well as business activity right from the beginning.[35]

Thus, technologies pose new challenges but could also help to hedge some risks. Identity theft occurs the world over, but it is more common in countries that lack a uniform system for identifying individuals, such as by ID card or document. This means that e-governance might actually reduce and not increase risks in this field. If we compare American laws on identity theft, studies have shown that technologies make such theft more difficult as criminals have a harder time attaining their desired goal.[36] On information systems, such measures include firewalls that restrict outside access, control network traffic, logical access rights and event logs to prevent unauthorised changes of data and so forth. Some of the measures safeguard against new risks that the technology itself has created. But it is also

[33] Examples http://ico.org.uk/what_we_cover/handling_complaints

[34] An example of such a study: "Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)" 18 July 2013.
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18_Smart_borders_EN.pdf

[35] For more about "privacy by design", see:
http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-estonian.pdf

[36] M. Anandarajan, R. D´Ovidio & A. Jenkins (2013) "Safeguarding consumers against identity-related fraud: examining data breach notification legislation through the lens of routine activities theory": *International Data Privacy Law* 2013 Vol. 3, No. 1 (51-60): p. 53.

possible to apply technology to make operations even more secure than they are in the "real world." But this attitude requires general mind-sets to change; for instance the e-voting system in widespread use in Estonia has not yet been adopted by many other countries.

The use of technologies and automated data processing may provide additional knowledge that would be impossible to gain otherwise; therefore, it could foil justified expectations regarding the extent and expedience of data processing. An illustration would be a person walking with friends down the street eating ice cream. Every passer-by could get information such as what the people are wearing, what brand of ice cream they are eating, who they are talking to, what they look like and what they are talking about. One must change one's behaviour if one wants to restrict access to such public information. Yet there is a justified assumption that there are no cameras or unrestricted view of what goes on in the bedroom (even in a hotel or rental) or changing room. The same principles must be applied in the electronic environment. Yet technologies such as facial recognition[37] can allow one to gain more information about people walking down the street than what can be seen in person. There must be analysis of whether such knowledge can violate privacy and if so, there should be a discussion about possible consequences. Such analysis has been conducted for years in both academic and general discourse, by corporations and to a certain extent by the court system, but it must be said that there is no generally accepted view of the boundaries of the use of technology.

Information technology has led to major changes in society in a number of fields, with the media being one of the most heavily influenced areas. For both newspapers and broadcasting and, more broadly, for journalism as a profession, the modern media and its immediacy and global reach has meant a completely new reality. It affects privacy in many ways, such as the fact that we can no longer rely on state control (broadcasting) or self-regulation (print, primarily) together with professional journalism ethics to create a framework of what can be shown or presented in the media and how. "Ordinary people" can distribute information in real time across the world at very low cost and with little effort. This could represent a boom for freedom of expression, as more and more information is reaching more people, but it also brings up – with greater urgency – situations in which freedom of expression and other fundamental rights and freedoms may be in conflict.

Due to technological advances, there are new main players with regard to the application of the existing rules. With regard to the media, we have already seen how the range of actors is much greater and less defined than just a few decades ago. In general, nearly every walk of life and a majority of the world's countries have experienced a change in the direction of a much greater role for the private sector. Internet service providers, who are essential to the functioning of much of modern society, are mainly private businesses. Key social networks are also privately owned. The IT situation is not unique, as in much of the world there is also much more private enterprise in the transport and energy sectors than there was 30 years ago. Private firms are generally more efficient, are able to adapt and innovate faster and more effectively, and offer more alternatives for individuals, so the trend is to be welcomed.

[37] For more about the dispute, see e.g.: http://www.theguardian.com/technology/2014/may/04/facial-recognition-technology-identity-tesco-ethical-issues.EU .

Yet, it also means challenges to the legal system, as it has to apply legal norms effectively in terms of corporate responsibility and be able to keep certain companies from becoming so powerful as to start impacting the entire market negatively, thereby eroding the same advantages that a market creates. The legal situation may be particularly complicated because large companies are often international and questions of jurisdiction arise.

All these topics mean that data protection and privacy protection is complicated in a modern, high-tech society and it is no wonder that much discussion is being devoted to it among politicians, academics, civil society and media figures. The debate also shows that there is no one answer or even clear directions. An interesting example was the EU court decision against Google and the "right to be forgotten" – the background here is privacy protection and a number of human rights co-organisations have been very critical, saying that it poses a threat to freedom of expression.

We must consider that people are not as knowledgeable as they should be in order to assess, accurately and over the long term, the data protection risks posed by social networks and modern technologies. That is why it is difficult to rely solely on people's own responsibility. Yet, it is also important not to overestimate what can be accomplished through legislation. The legal system can be used to establish frameworks for corporate responsibility and create certain conditions for their activity so that it would be as safe as possible, ensuring that, should anything go wrong, there would be measures to deal with it. But laws, along with official oversight, are just one part of the whole. The big picture undoubtedly also includes a new way of assessing privacy: while modern technology need not mean the end of privacy, it will certainly mean a re-evaluation.