Protection of Personal Data and its status as a Fundamental Right -

In the scope of International Law and EU Law

University of Turku
Faculty of Law
Master's Thesis
Monica Hagsberg, 507201
Spring 2019

Abstract

UNIVERSITY OF TURKU
Faculty of Law

MONICA HAGSBERG: Protection of Personal Data and its status as a Fundamental Right – In the scope of International Law and EU Law
Master's Thesis, p. 65
International Law
05/2019
According to the rules of the University of Turku, the originality of this thesis has been checked with the Turnit Originality Check system.

Personal data protection has raised discussion during the recent years both in international and national level. With the development of technology, internationalism and the economy it is more and more important to protect the personal data. The adequate way to protect the personal data needs to be considered thoroughly; should it be protected with secondary legislation or with fundamental legislation?

During the recent years, the personal data protection legislation in both international and national level has increased. Despite this, the protection of personal data faces threads and challenges every day. These threads and challenges emerge from the inconsistency of international and national data protection legislations, from terrorism and crime, and from the economic and technological development. Also the collisions between different fundamental rights are challenging. For instance, it is not always easy to assess the order of importance between the personal data protection and the right to free flow of data.

In this thesis I shall research the status of personal data protection in international level and in international jurisdiction. I will start my research by assessing the threads and challenges personal data protection faces every day. I shall then take a closer look into the relevant European Union law and then to international law. I shall also make a slight comparison between the EU law and the international law. My goal is to figure out the actual challenges and threads to personal data protection and, also, the legal protection that personal data needs and already has. I believe I have reached this goal.

I believe that the personal data should be protected as a fundamental right, but it hasn't reached this status in international level yet. For the data protection to reach this status as a fundamental right, international legislations and regulations needs to be revised.

My research methods have mostly been legal dogmatic. My research is mainly based on the relevant legal literature, sources of laws and other written legal sources. The empiric parts in this thesis are mainly from the author herself.

Keywords: personal data protection, human rights, fundamental rights, internationalism, the European Union, the United Nations, technology, economy, terrorism, crime

Tiivistelmä

TURUN YLIOPISTO
Oikeustieteellinen tiedekunta

MONICA HAGSBERG: Protection of Personal Data and its status as a Fundamental Right – In the scope of International Law and EU Law
Pro gradu –tutkielma, s. 65
Kansainvälinen oikeus
05/2019
Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin Originality Check -järjestelmällä.

Henkilötietosuoja on puhututtanut viime vuosina sekä kansainvälisellä että kansallisella tasolla. Teknologisen kehityksen, kansainvälistymisen sekä taloudellisen kehityksen myötä henkilökohtaisen tiedon suojaaminen on entistä tärkeämpää. Siksi onkin pohdittava, miten henkilötietosuoja voidaan turvata parhaiten; tavallisella lailla vai ihmisoikeustason lainsäädännöllä?

Viime vuosina henkilötietosuojaa koskeva lainsäädäntö on lisääntynyt niin kansainvälisellä kuin myös kansallisella tasolla. Tästä huolimatta henkilötietosuojan turvaaminen on uhattuna päivittäin. Näitä uhkia aiheutuu niin kansainvälisen ja kansallisen lainsäädännön epäjohdonmukaisuuksista, rikollisuudesta ja terrorismista kuin myös taloudellisesta kehityksestä. Oikeuksien yhteentörmäys on myös haasteena, kun esimerkiksi punnitaan tärkeysjärjestystä henkilötietosuojan ja tiedon vapaan liikkuvuuden välillä.

Tässä tutkielmassa tarkastelen henkilötietosuojan asemaa kansainvälisellä tasolla ja kansainvälisessä oikeusjärjestelmässä. Aloitan tutkimuksen tarkastelemalla henkilötietosuojan kohtaamia uhkia. Uhkien kautta tarkastelen ensin Euroopan Union oikeutta, josta jatkan kansainväliseen oikeuteteen sekä näiden kahden vertailuun. Tavoitteenani tässä tutkielmassa on havaita henkilötietosuojan kohtaamat todelliset uhat sekä sen tarvitsema ja saama oikeudellinen suoja. Mielestäni olen tähän tavoitteeseen päässyt.

Mielestäni henkilötietosuoja tulisi olla ihmisoikeus ja se tulisi säätää selkeästi kaikkiin kansainvälisiin ja myös kansallisiin ihmisoikeuskokoelmiin. Henkilötietosuoja ei ole vielä saavuttanut ihmisoikeusasemaa kansainvälisellä tasolla ja saavuttaakseen tämän tason tulisi kansainvälisiä ihmisoikeuskokoelmia uudistaa.

Tutkimuskeinoina tässä tutkielmassa on enemmälti käytetty oikeusdogmaattista tutkimusta perehtyen oikeuskirjallisuuteen ja lainsäädäntöön sekä muuhun relevanttiin kirjalliseen aineistoon. Empiiriset näkökulmat tutkimukseen on lähinnä tulleet kirjoittajalta itseltään.

Asiasanat: henkilökohtainen tietosuoja, ihmisoikeudet, perusoikeudet, kansainvälisyys, Euroopan Unioni, Yhdistyneet Kansakunnat, teknologia, talous, terrorismi, rikollisuus

Contents

Abstract II

Abstract in Finnish III

Table of contents IV-V

Sources VI-XI

Table of abbreviations XII

Table of Contents

1. Introduction.....1

1.1. The theme.....1

1.2. Research questions, methodology and methods.....5

2. The challenges for personal data protection in the 21st century.....11

2.1. Internationalism and culture.....11

2.2. Technology.....15

2.3. Terrorism and crime.....16

2.4. Economy.....21

3. Protection of personal data in Europe and in the European Union law.....26

3.1. Fundamental rights and human rights.....26

3.1.1. The two statutes: European Convention on Human Rights (ECHR) and The Charter of Fundamental Rights of the European Union (CFREU).....26

3.1.2. Fundamental and human right status theories.....29

3.2. The European Union regulation on data protection.....32

3.2.1. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data...32

3.2.2. The General Data Protection Regulation (GDPR).....35

3.3. Case studies.....37

4. Protection of personal data in international law.....44

4.1. The United Nations (UN).....44

4.1.1. About the United Nations.....44

4.1.2. The Universal Declaration of Human Rights (UDHR).....46

4.1.3. The International Covenant on Civil and Political Rights (ICCPR).....47

4.2. Guidelines from international organizations……48
4.2.1. United Nations Human Rights Council (HRC)……48
4.2.2. The Organization for Economic Co-operation and Development (OECD)……49
4.2.3. Others……52
4.3. International human rights law……53
4.4. The European Union law vs. international law……56
5. Conclusions……60

Sources

Bibliography

Antikainen, Antti; Risk-based approach as a solution to secondary use of personal data. Pro gradu, Helsinki 2014.

Beyond data protection: strategic case studies and practical guidance; ed. Ismail, Noriswadi – Yong Cieh, Edwin Lee. Springer 2013.

Bilder, Richard B.; An Overview of International Human Rights Law (Guide to International Human Rights Practice, p. 3-18). 2016.

Blume, Peter; Introduction (Nordic data protection law, p. 1-9). 2001.

Boehm, Franziska; Information sharing and data protection in the area of freedom, security and justice – Towards harmonized data protection principles for information exchange at EU-level. Springer 2012.

Brkan, Maja; The Court of Justice of the EU, Privacy and Data Protection: Judge-made law as a leitmotif in fundamental rights protection (Courts, privacy and data protection in the digital environment, p. 10-31). 2017.

Bygrave, Lee A.; Data protection law: approaching its rationale, logic and limits. The Netherlands 2002.

Caloyannides, Michael A.; Privacy protection and computer forensics. Boston 2004.

Chester, Jeff; Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the "Big Data" Era (European Data Protection: In Good Health?, p. 53-77). 2012.

Colonna, Liane; Legal implications of data mining – Assessing the European Union's data protection principles in light of the United States government's national intelligence data mining practices. Tallinn 2016.

Courts, privacy and data protection in the digital environment; ed. Brkan, Maja – Psychogoipoulou, Evangelia. Edward Elgar Publishing 2017.

Data protection on the move; current developments in ICT and privacy/data protection; ed. Gutwirth, Serge – de Hert, Paul – Leenes, Ronald. Springer 2016.

De Busser, Els; The Adequacy of an EU-US Partnership (European Data Protection: In Good Health?, p. 185-202). 2012.

De Hert, Paul – Gutwirth, Serge; Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action (Reinventing data protection?, p. 3-44). 2009.

European Data Protection: Coming of Age; ed. Gutwirth, Serge – de Hert, Paul – Leenes, Ronald – Poullet, Yves. Springer 2013.

European data protection: in good health?; ed. Gutwirth, Serge – de Hert, Paul – Leenes, Ronald – Poullet, Yves. Springer 2012.

Flaherty, David H.; Data protection and national information policy (From data protection to knowledge machines: the study of law and informatics, p. 29-44). 1990.

Friedewald, Michael – Lieshout, Mar van – Rung, Sven – Ooms, Merel; The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security (Data protection on the move; current developments in ICT and privacy/data protection, p. 55-73). 2016.

From data protection to knowledge machines: the study of law and informatics; ed. Seipel, Peter. Oslo 1990.

González Fuster, Gloria; The emerge of personal data protection as a fundamental right of the EU. New York, Springer 2014.

Graef, Inge; EU competition law, data protection and online platforms – Data as essential facility. Wolters Kluwer 2016.

Greenleaf, Graham W.; Asian data privacy laws: trade and human rights perspectives. Oxford 2014.

Guide to International Human Rights Practice; ed Hannum, Hurst. Pennsylvania 2016.

Hakapää, Kari; Uusi kansainvälinen oikeus. Helsinki 2010.

Hannum, Hurst; Implementing Human Rights: An Overview of Strategies and Procedures (Guide to International Human Rights Practice, p. 19-38). 2016.

Heisenberg, Dorothee; Negotiating privacy: the European Union, the United States and personal data protection. Lynne Rienner Publishers 2005.

Kiss, Attila – Szke, Gergely László; Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation (Reforming European data protection law, p. 227-241). 2015.

Koillinen. Mikael – Kulla, Heikki; Julkisuus ja henkilötietojen suoja viranomaistoiminnassa. Turku 2014.

Kosta, Eleni; Consent in European data protection law. The Netherlands 2013.

Kowalik-Banczyk, Krystyna; The clash between protection of personal data and protection of intellectual property rights in internet in the CJEU jurisprudence (Lawyers in the media society: the legal challenges of the media society, p. 142-152). 2016.

Kremer, Jens; The end of freedom in public places?: privacy problems arising from surveillance of the European public space. Helsinki 2017.

Lawyers in the media society: the legal challenges of the media society; ed. Saarenpää, Ahti – Sztobryn, Karolina. Rovaniemi 2016.

Léonard, Laura – Skouma, Georgia; On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection (Reforming European data protection law, p. 42-58). 2015.

Lewis-Anthony, Siân; Treaty-based Procedures for Making Human Rights Complaints Within the UN System (Guide to International Human Rights Practice, p. 41-59). 2016.

Lynskey, Orla; From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis (European Data Protection: Coming of Age, p. 59-84). 2013.

Länsineva, Pekka – Pentikäinen, Merja; Ihmisoikeudet, perusoikeudet ja vastuullinen yritystoiminta. Turku 2011.

Markou, Christiana; The 'Right to Be Forgotten': Ten Reasons Why It Should Be Forgotten (Reforming European data protection law, p. 154-169). 2015.

Neuvonen, Riku – Rautiainen, Pauli; Perusoikeuksien tunnistaminen ja niiden sisällön määritteleminen Suomen perusoikeusjärjestelmässä. Lakimies 1/2015, s. 28-53.

Newman, Abraham L.; Protectors of privacy: regulating personal data in the global economy. Ithaca 2008.

Newton, Lee; Facebook nation: total information awareness. New York, Springer 2014.

Nordic Data Protection; ed. Blume, Peter. DJOF Publishing Copenhagen 2001

Organisation for Economic Co-operation and Development; Guidelines on the protection of privacy and transborder flows of personal data. Paris 1981.

Pagallo, Ugo; On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law (European Data Protection: In Good Health?, p. 332-346). 2012.

Psychogiopoulou, Evangelia; The European Court of Human Rights, Privacy and Data Protection in the digital era (Courts, privacy and data protection in the digital environment, p. 32-62). 2017.

Reforming European data protection law; ed. Gutwirth, Serge – de Hert, Paul – Leenes, Ronald. Springer 2015.

Reinventing data protection?; ed. Gutwirth, Serge – de Hert, Paul – Nouwt, Sjaak – Poullet, Yves – de Terwange, Cécile. Springer cop. 2009.

Rodotà, Stefano; Data Protection as a Fundamental Right (Reinventing data protection?, p. 77-82). 2009.

Selmer, Knut S.; Data protection policy (From data protection to knowledge machines: the study of law and informatics, p. 11-28). 1990.

Tapani, Jussi; Rikosvastuun perusteet. Turku 2013.

Terwangne, Cécile de; Is a Global Data Protection Regulatory Model Possible? (Reinventing data protection?, p. 175-189). 2009.

Tzanou, Maria; The fundamental right to data protection: normative value in the context of counter-terrorism surveillance. Hart Publishing 2017.

Ustaran, Eduardo; The Scope of Application of EU Data Protection Law and Its Extraterritorial Reach (Beyond Data Protection: Strategic Case Studies and Practical Guidance, p. 135-156). 2013.

Wong, Rebecca; Data security breaches and privacy in Europe. London 2013.

Cases

Court of Justice of the European Union

Case C-207/16 *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788

Case C-275/06 *Promusicae* [2008] ECLI:EU:C:2008:54

Joined Cases C-293/12 *Digital Rights Ireland Ltd* and C-594/12 *Kärntner Landesregierung* [2014] ECLI:EU:C:2014:238

European Court of Human Rights

Klass and others v Germany App no. 5029/71 (ECtHR, 6 September 1978)

Perry v the UK App no. 63737/00 (ECtHR, 17 July 2003)

S. and Marper v the UK App nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008)

Internet sources

China Daily; 6 cultural differences between China and the US, 1.4.2015. http://www.chinadaily.com.cn/opinion/2015-04/01/content_19834344_6.htm, read 21.3.2018.

CSO (Taylor Armerding); The 17 biggest data breaches of the 21st century, 26.1.2018. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, read 21.3.2019.

European Commission; Why do we need the Charter? – The Charter of Fundamental Rights, what it covers and how it relates to the European Convention on Human Rights. https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_fi, 22.3.2018.

EU GDPR; GDPR Key Changes. https://eugdpr.org/the-regulation/, read 21.5.2019.

National Public Radio, NPR (Curt Nickisch); Boston Marathon Surveillance Raises Privacy Concerns Long After Bombing. https://www.npr.org/2015/04/17/400164221/boston-marathon-surveillance-raises-privacy-concerns-long-after-bombing?t=1553158085133, read 21.3.2019.

OECD; About the OECD. http://www.oecd.org/about/, read 27.3.2019.

OHCHR; United Nations Human Rights Council. https://www.ohchr.org/EN/HRbodies/HRC/Pages/Home.aspx, read 26.3.2019.

United Nations; About the UN – Main Organs. https://www.un.org/en/sections/about-un/main-organs/index.html, read 26.3.2019.

United Nations; About the UN – Overview. http://www.un.org/en/sections/about-un/overview/index.html, read 26.3.2019.

United Nations; Charter of the United Nations. http://www.un.org/en/sections/un-charter/introductory-note/index.html, read 26.3.2019.

Sources of law

Charter of Fundamental Rights of The European Union, 2012/C 326/02, 26.10.2012.

Constitution of Finland, 11.6.1999/731.

Convention on the Organization for Economic Co-operation and Development, 14.12.1960.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24.10.1995.

European Convention on Human Rights, 4.11.1950.

General Data Protection Regulation, 2016/679, 4.5.2016.

International Covenant on Civil and Political Rights, 23.3.1976.

Report of the Human Rights Council, A/70/53, 27.3.2015.

Report of the Human Rights Council, A/72/53, 23.3.2017.

Treaty of Lisbon, 2007/C 306/01, 17.12.2007.

Universal Declaration on Human Rights, 10.12.1948.

Other

OECD; Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines / OECD Digital Economy Papers No. 229. OECD Publishing, Paris 2013.

Table of abbreviations

CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DPA	Data Protection Authorities
ECtHR	European Court of Human Rights
ECHR	European Convention on Human Rights
EU	European Union
GDPR	General Data Protection Regulation
HRC	United Nations Human Rights Council
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
NGO	Non-governmental Organization
NATO	North Atlantic Treaty Organization
OECD	The Organization for Economic Co-operation and Development
TEU	Treaty of the European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UN	United Nations

1. Introduction

1.1. The theme

In 2013 and 2016 a website called Yahoo was attacked by criminal hackers.[1] Personal data, including names, email addresses, telephone numbers and dates of birth, of over 3 billion users fell into the hands of criminal hackers.[2] Also in 2016 the database of a website called Adult Friend Finder was hacked when the hackers stole personal data, including names, email addresses and passwords, of over 410 million users.[3] In 2014 it was eBays turn, when criminal hackers got their hands into personal data, for example names, addresses, dates of birth and passwords, of approximately 145 million eBay users.[4] These are only few examples of the worst data breaches in the 21st century.[5] During these modern and developed times, data breaches happen daily causing huge privacy and, also, economic problems.[6]

Protection of personal data, which is usually described as any data that can be used to identify a person,[7] and data breaches are not only the 21st century's problem. Personal data protection has raised discussion and thoughts for at least 30 years. For instance, the council of the Organization for Economic Co-operation and Development (OECD) recognized already in the 1980s the need to react on the issues and problems relating to the protection of privacy and personal data including issues evolving from the cross-border flows of data.[8] The council of the OECD compiled a written document of recommendations and guidelines concerning these issues in order to improve the cohesion of legislation of the OECD member states, to clarify the importance of protecting personal data and, at the same time, to make sure that free flow of all possible information and data is secured.[9] The discussion about personal data protection seems to have increased,

[1] *CSO,* https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, read 4.3.2018.
[2] *Ibid.*
[3] *Ibid.*
[4] *Ibid.*
[5] *Ibid.*
[6] *Ibid.*
[7] *Kowalik-Banczyk* 2016, p. 143.
[8] *OECD* 1981, p. 7.
[9] *Ibid.*

which is not a surprise considering the modern development in technology, internationalism and the issues evolving from these developments.

With the development of technology and the trend of using technology as a device for handling personal data, the protection of personal data has become more and more important. This can be indicated with the new legislations, such as the General Data Protection Regulation (GDPR), and with the recent legal praxis. The amount and importance of cases that concern the fundamental rights to privacy and protection of personal data has increased in the Court of Justice of the European Union (CJEU) and in the European Court of Human Rights (ECtHR) during recent years.[10]

However, technology and its development is not the only challenge for the protection of personal data. Terrorism and internationalism, with the help of technology, can also be considered as threads for the protection of personal data. A hacker can be a terrorist, who in addition to conducting data breaches, have also terroristic intentions. In these situations, when terrorism is in involved, national security usually prevails over data protection.[11] For instance in terrorist attacks, policy makers of a nation do the necessary measures in order to maintain the national security and not for the personal data protection of an individual.[12] Internationalism has figuratively shrunken the world and many issues, for instance data protection issues, concern many nations at the same time. One terroristic or other criminal data breach may be a problem for multiple nations. Threads to the protection of personal data are not always criminal and, for instance, sudden collapses of databases with personal data may cause severe damage to the data subjetcs, whose personal data has been exposed or abused.

To answer to these threads, there are internationally many laws, provisions, conventions, treaties and constitutions that concern the protection of personal data. These different international laws, provisions, conventions, treaties and constitutions differ from each other and they may give very diverse statuses for the protection of personal data. For instance, this sort of divergence may already

[10] *Brkan* 2017, p.10.
[11] *Newman* 2008, p. 123-124.
[12] *Ibid*.

be seen in the EU level. In the 8th Article of the Charter of Fundamental Rights of the European Union (CFREU), the protection of personal data has been legislated as a fundamental right. However, in the national constitutions, for instance in the Finnish constitution, the protection of personal data has not specifically been legislated as a fundamental right. The legislation gets even more inconsistent in the international level. For instance, even the Universal Declaration of Human Rights (UDHR) does not have a specific article for the protection of personal data. The reason for this might the fact that the UDHR is very universal by its nature and sets mainly the guidelines for all the people and all the nations.

In legal theories, personal data and data in generally are continuously being assessed from various different angles, which lead to multiple outcomes. One viewpoint is that individuals own their personal data and that personal data is in a way a commercial good.[13] It has also been described as a new currency.[14] In practice this means that companies who sell and distribute, for instance, movies and series in digital form, could ask their customers to give compensation either in money or to provide personal data or other data as a compensation.[15] This is more of a private law viewpoint to data protection, which is insufficient in Europe.[16] In Europe the data protection ideology adapts the public law principles and, also, assesses the relationship between private and public law.[17] More specifically, according to the European data protection theory, the controlling of intellectual asymmetry is the key with data protection.[18] Because of the intellectual asymmetry, there are now certain principles that balance the uneven relationship between the individuals and the public power, which gives protection against misuses of someone's personal data by the public power and other individuals.[19]

The question about the status of personal data protection hasn't clearly been stated in the sources of law, the legal theories, the legal praxis and the legal literature. Antti Antikainen writes in his thesis that protection of personal data is a

[13] *Koillinen – Kulla* 2014, p. 109.
[14] *Graef* 2016, p. 126.
[15] *Ibid.*
[16] *Ibid.*
[17] *Koillinen – Kulla* 2014, p. 110.
[18] *Ibid.*
[19] *Ibid.*

fundamental right.[20] However, he does not make a distinction between privacy and personal data protection.[21] Legal scholar Mikael Koillinen thinks also that the data protection is an independent fundamental right.[22] Koillinen reasons this by stating that even though roots of the data protection are in the right to privacy, data protection is not only a part of the protection of privacy.[23] This insight of seeing the data protection as an independent human right has not been fully accepted within all legal scholars.[24] For instance, professor Veli-Pekka Viljanen sees data protection as an integral part of the fundamental right to privacy.[25]

Fundamental and human rights are the ground rules and are in the core of the international and national jurisdictions.[26] They are described as rules and norms that form the base for the whole judicial system.[27] However, the status of fundamental and human rights is not that simple. When interpreting international fundamental and human rights, it is required to also consider national conditions and culture and how they affect on the status of fundamental and human rights.[28] This can be seen, for instance, from the jurisdiction of European Court of Human Rights (ECtHR) when it interprets the European Convention on Human Rights (ECHR).[29] I shall get back to jurisdiction of ECtHR later in this thesis.

Currently data protection is in some sort of a turning point. Legal theories, legal literature and sources of laws of data protection evolve continuously. One good example is the new European Union (EU) General Data Protection Regulation (GDPR), which came into force in May 2018. There is an accurate need for the development of data protection legislations and regulations and for the protection of personal data. Data breaches and misuses of personal data happen globally, daily and in different ways. The few examples of these different ways are the spying of the telecommunications of individuals done by the National Security

[20] *Antikainen* 2014, p. 1.
[21] *Antikainen* 2014*,* p. 17.
[22] *Neuvonen – Rautiainen* 2015, p. 34.
[23] *Ibid.*
[24] *Ibid.*
[25] *Ibid.*
[26] *Neuvonen – Rautiainen* 2015, p. 28.
[27] *Ibid.*
[28] *Neuvonen – Rautiainen* 2015, p. 44.
[29] *Ibid.*

Agency (NSA) in the United States[30], the viewing of information concerning the death of a famous skier in Finland done by the policemen[31] and the collecting of personal data of customers while they are joining a regular customer systems done by different stores[32] Nevertheless, the question about the need for protection of personal data is not unclear. Instead, the question about the manner of protection is under debate; how the personal data is protected and how it should be protected. Currently the personal data protection is seen as an independent fundamental right[33] as well as a part of the fundamental right to privacy[34] and, also, not as a fundamental right at all. In this thesis I chose one of these viewpoints and I am going to research, whether the personal data protection is an independent fundamental, or human, right.

1.2. Research questions, methodology and methods

Fundamental rights and human rights have priority in many national and international legal systems. In the Article 30 of the United Nation's (UN) Universal Declaration of Human Rights, it has been stated that none of the enacted rights can be made null and void by any interpretation, performance or act. There are very similar Articles in the EU legal order, more specifically, in the Treaty of the European Union (TEU), in the European Convention on Human Rights (ECHR) and in the Charter of Fundamental Rights of the European Union (CFREU). In these EU regulations, it has been enacted that the fundamental and human rights can only be restricted by law and even then, in a reasonable and necessary way. This has, of course, had effect on the EU member states legislation, including Finland, and on the interpretation in situations, where there is a collision between the constitution and the regular legislation. In these situations, at least in Finland, the regular legislation is being interpreted in a way that is favorable to the fundamental and human rights or, if that is not possible, fundamental and human rights prevail over

[30] *Koillinen – Kulla* 2014, p.101.
[31] *Ibid.*
[32] *Ibid.*
[33] *Koillinen – Kulla* 2014, p.102.
[34] *Koillinen – Kulla* 2014, p.117.

regular law.[35] In Finland, there is also a specific list of guidelines concerning the restriction of fundamental and human rights, which has mainly been crafted according to above-mentioned EU charters. The Finnish national guidelines for restricting fundamental rights are as follows:

- Restrictions must be provided by the law.
- Restrictions must be precise and accurately defined.
- Restrictions must be required by a cogent social need.
- The core of a fundamental right cannot be restricted by a regular law.
- The essence of a human right cannot be a subject to restrictions.
- The legislator must secure the legal protection of a right despite possible restrictions.
- Restrictions cannot collide with international human rights commitments.[36]

These above-mentioned charters, conventions and treaties have listed the enacted fundamental and human rights and, also, clarified the international status of fundamental and human rights. Because of the content and the purpose of these charters, conventions and treaties, I believe that the fundamental and human rights belong inseparably to every people around the world.

However, the existence of fundamental rights and human rights and their internationally acknowledged importance does not mean that everyone around the world benefits or even wants to benefit from fundamental and human rights. There are, of course, cultural differences all around the world, which affect to the status of fundamental and human rights in different territories. For instance, the Finnish culture and the Chinese culture differ from each other quite a lot. It is obvious that the Finnish culture is familiar to me, because I have lived in Finland my whole life. The Chinese culture, however, became familiar to me during my previous studies in law school. I have studied it and its relation to fundamental and human rights while doing my bachelor's degree in law. In Finland the individual rights are important. In China, on the other hand, the family has priority and collective,

[35] *Länsineva – Pentikäinen* 2011, p. 5.
[36] *Tapani* 2013, p. 30-31.

family orientated rights matter more than individual rights.[37] This obviously affects to the status of individual rights.[38] This may also be seen in the legal praxis of China.[39] The Chinese constitution may not be applied directly in courts and, to be more specific, an individual cannot raise a case in civil disputes for misusage or breach of his or hers constitutional right.[40] Again this differs from the legal praxis in Finland and, also, from the legal praxis in the EU, where it is possible for an individual to file a petition in a breach of his or hers fundamental or human right.[41]

Despite the cultural differences all around the world, I still believe that fundamental and human rights should be respected and prioritized in all legal systems, especially the compulsory provisions such as the right to live. I believe that the fundamental rights, which have priority in a legal system, give individuals more security and, when these rights are respected, also a more secure position of having protection against other individuals and governmental power. I think that each fundamental right is important and should be respected. However, it is clear that sometimes fundamental and human rights collide with each other, which leads to an inevitable situation, where a fundamental right needs to be restricted in order for the other fundamental right to have its force. In these situations, the right solution is to aim for the most harmless outcome.

The ideology of the importance of fundamental and human rights has guided me with my research. I am interested in fundamental and human rights and I am willing to figure out how these are respected nationally and internationally and, also, what are the reasons for respecting or unrespecting these rights. The lists of fundamental rights may vary in different treaties and constitutions, but principally fundamental rights are quite the same all over the world. There might also be some differentiations between the terms fundamental right and human right. However, according to the observations I have made from the international charters, the differences do not seem relevant and in this thesis, I am going to use them as synonyms. The lists of fundamental rights, as well as lists of human rights, cover

---

[37] *China Daily,* http://www.chinadaily.com.cn/opinion/2015-04/01/content_19834344_6.htm, read 21.3.2018.
[38] *Ibid.*
[39] *Ibid.*
[40] *Greenleaf* 2014, p. 197.
[41] *Hakapää* 2010, p. 164.

many fields of an individual's life. For instance, the rights to privacy, to reasonable income and to non-discrimination are only few examples of the fundamental rights listed in the Finnish constitution, in the Charter of Fundamental Rights of the EU and in the Universal Declaration of Human Rights. For this research, I wanted to concentrate on one fundamental right and I decided to focus on the protection of personal data. I ended up to this decision, because to me the status of personal data protection is unclear and the discussion around it seems to be growing.

In this thesis, I am researching the current status of the protection of personal data, its challenges and its future prospects. Particularly, I am researching its status as a fundamental right. My research questions have formed into one main question, which is supported with two additional questions. The main research question is; can the protection of personal data be seen as a fundamental right? The supportive questions are as follows:

- How can or cannot the protection of personal data be seen as a fundamental right? Why should or should not the protection of personal data be seen as a fundamental right?

- What are the 21st century's threads for protecting individual's personal data?

I am researching these questions under the scopes of EU law and international law and, also, by comparing these two scopes of law.

In order to figure out, whether the protection of personal data can be seen as an universal and as an independent fundamental right, is a thorough research of national and international laws, provisions, legal literature and tribunal cases required. However, even with a thorough research, it might be impossible to figure out the 100% universal ideology behind the status of personal data protection. However, I still believe it is possible to make some conclusions of the general, universal view in this matter.

The legal dogmatic method is the prior method that I am applying in this research. The readings in legal literature and articles, laws, treaties and conventions have led this research onwards. Also, I have made myself familiar with the general opinion on the protection of personal data and its current status by reading different news articles and by observing people's reaction to the discussion about the protection of personal data. It seems like people are concerned, because they are unaware about where their personal data may have spread to, for instance, through social media and mobile phones. However, the level of concern is not that frightening that it would make people to stop using social media and other digital platforms.

With this research, I am not only educating myself, but also trying to accelerate the discussion around the protection of personal data. Because of its style and nature, this research is primarily directed to legal scholars. However, it would be ideal if this research also woke the interests of regular people and, because of its importance and its current nature, I am directing this research to both regular people and legal scholars and also to both individuals and organizations.

I shall start my research in the next chapter by exploring threads and challenges that protection of personal data faces. I will go through four different types of threads with the help of legal literature. Chapters three and four are for the EU and international legal aspects, but in order for this research to be as explicit as possible, I will address the aspects of EU law and international law in their own chapters. In the third chapter, I shall address protection of personal data in the scope of EU law with the help of the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights, the new General Data Protection Regulation and also the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which applied before the General Data Protection Regulation was adopted. The fourth chapter has been dedicated for the to international law and in this chapter I shall address the protection of personal data in the light of the Universal Declaration on Human Rights and with the help of different guidelines given by international organizations. Finally, the fifth chapter

is the concluding part, where I will make some conclusions of this research and suggestions for the improvement of international data protection legislations.

2. The challenges for personal data protection in the 21st century

2.1. Internationalism and culture

As we all know, the population of the globe increases every year. However, in a way, the world has decreased. Nations' borders have grown dimmer when trespassing of people, goods and data is more frequent and made easier and easier. The world has faced a series of changes during the last ten years.[42] During these years, there has been a massive development in technological, economic and social issues and this development process is still going on.[43] While these developments and changes can be seen as positive issues, are they almost always linked to different kinds of challenges.

Protection of personal data faces challenges and threads every day. While researching this topic, I believe that the main challenges for protection of personal data in the 21st century originate from the development of technology, the worldwide terrorism, the internationalism and different cultures, and also the inconsistency of international and national legislations and regulations. This is not an exhaustive list of the challenges that the protection of personal data faces, but these are the threads in which I am going to focus on in this thesis. All these listed challenges have effect on each other and may take place at the same time, yet I shall still address them as separate threads starting with internationalism, cultural issues and inconsistency of international and national legislations and regulations.

Internationally there are probably hundreds of millions of internet and social media users, who use different international websites and social media browsers. It is quite easy for an internet user to store personal information on a website with only few clicks.[44] Even though the storing of personal data is easy, deleting it from the internet is not that easy.[45] It is commonly known fact that once you post or store something to the internet, for instance photos or other personal information, there is a risk that it will spread all over the internet, as well as all over the world,

[42] *Kiss – Szke* 2015, p. 235.
[43] *Ibid.*
[44] *Markou* 2015, p. 157.
[45] *Ibid.*

and it might be really difficult to delete the stored data from everywhere it has spread to. This of course might raise concern within the people, who have stored their personal information on internet. Other internet users, hackers and, also, those, who maintain digital personal data registers, may abuse photos and other personal data stored into the internet.[46] This kind of abuse may cause serious damage for the data subject.[47]

Researches have been made about how do the internet users feel about their privacy and data protection while using Internet in different countries and using websites originated from different countries.[48] According to the results of these researches, most of the Internet users think that their privacy and personal data are under a continuous threat and they fear that their privacy and personal data will be breached.[49] However, the level of fear is not sufficient enough to change the manners and amount the Internet use, at least on my opinion. Nevertheless, people are different and people think differently about privacy and data protection issues; some think that privacy and data protection are very important while others don't[50] and some people see privacy and data protection breaches and violations as more serious than others.[51] For instance, when in some cultures personal data can be seen as a highly private data, in some cultures the same personal data is not seen as private at all.[52] As I mentioned before, I have researched slightly the Chinese culture and the cultural differences between China and Finland give a good example for this; in Finland data protection and privacy is very important to individuals when in China the community's rights are more important than individuals privacy and data protection. This speaks for the cultural differences around the world, which affect on the contents of international provisions and, also, the way they are interpreted in different nations.[53]

These different approaches to privacy and data protection complicates the standardizing of international and national provisions and legislation on privacy

[46] *Selmer* 1990, p. 25.
[47] *Ibid.*
[48] *Kiss – Szke* 2015, p. 229.
[49] *Ibid.*
[50] *Heisenberg* 2005, p. 14.
[51] *Ibid.*
[52] *Heisenberg 2005, p. 13.*
[53] *Ibid.*

and data protection.[54] As stated before, in both international and national level the inconsistency of legislation is one of the challenges for data protection.[55] There are differences in regulations in the international level and, also, in national legislations and provisions concerning privacy and data protection regulations.[56] For instance, some nations have privacy and data protection regulations that concern both public and private sectors and some nations have privacy and data protection regulations concerning only the public sector.[57] In addition, international privacy and data protection regulations are interpreted differently in different legal systems[58] and aren't usually legally binding nor accurate by their nature.[59] For this reason, it is clear that issues relating to privacy and data protection in international relationships may be problematic.

The inconsistency in international and national legislation also affect negatively on the free flow of data.[60] As stated before, the cross-border flow of data has increased throughout the years within the development of technology and international economy.[61] Nations all around the world have encountered this increase and have wondered, how to maintain the balance between privacy and data protection and also the free flow of data.[62] Because the cross-border flows of all kinds of data has increased, the need for international co-operation and consistent legislation in data protection on international level has remarkably increased.[63]

In addition to the increase of data flows, the international co-operation in privacy and data protection is needed because of their status and cruciality in other types of international relationships.[64] In this modern world, which is international, hectic, highly technological and full of different cultures, national jurisdiction is not sufficient enough for controlling the international relationships, which is why

[54] *Heisenberg* 2005, p. 14.
[55] *Ibid.*
[56] *Newman* 2008, p. 43.
[57] *Ibid.*
[58] *Heisenberg* 2005, p. 13.
[59] *Heisenberg* 2005, p. 14.
[60] *OECD* 1981, p. 15.
[61] *Ibid.*
[62] *Newman* 2008, p. 43.
[63] *Colonna* 2016, p. 127.
[64] *Colonna* 2016, p. 403.

international provisions or legislations are needed to ensure the international privacy and data protection as well as the free flow of data.[65] In addition, the increased international trade and the global financial markets require international provisions on privacy and data protection issues.[66]

Coherent international data protection is not easy to achieve. As stated above, there are cultural differences, which affect on national and international jurisdiction. One challenge has also been the progress of data protection legislation on different national levels.[67] Many of the Western countries have struggled with data protection and privacy legislations and their status's, because they are connected to other important fundamental and human rights, such as the right to the freedom of speech.[68]

During the recent years, there has been some signs of international co-operation and standardizing of international data protection regulations and it can be said that the European Union has had the main role in the current international data protection standards.[69] Actually, the EU has basically created these standards and regulations by itself without any international co-operation.[70] Despite this slight development, there are still nations, like Japan, Australia and India, that, instead of complying with the standards and regulations set by the EU, have their own national data protection regulations.[71]

All in all, it is obvious that internationalism and cultural differences pose a serious challenge for data protection internationally and nationally. What can or cannot be done with personal data when it falls from one national area of jurisdiction to another? What kind of legal protection can an individual get, when the person who has abused his or her personal data, is from another country, where there is completely different culture and jurisdiction in data protection? These questions have an international viewpoint, yet they are closely connected to technology and

[65] *Colonna* 2016, p. 403.
[66] *Newman* 2008, p. 5.
[67] *Flaherty* 1990, p. 42-43.
[68] *Ibid.*
[69] *Heisenberg* 2005, p. 103.
[70] *Ibid.*
[71] *Heisenberg* 2005, p. 120.

its development, which is why I shall address the challenges that technology and its developments pose on the data protection.

2.2. Technology

Technology, especially information technology, has been developing all the way from the 1950s, when the so-called computer age begun.[72] With these developments, multiple different possibilities to, for instance, having access to personal data have occurred.[73] Computers, mobile phones and the internet are extremely popular and people all around the world use these frequently.[74] This is one reason for why international and national data protection legislations have been regulated during the recent years.[75]

The technological equipment have developed by external features; from a computer sized of a room to a laptop you can put in your bag and from a mobile phone bigger than your head to a mobile phone that you can put in your pocket. Another development has happened with the usability of these equipment. Today's computers and mobile phones have high technical capabilities.[76] For instance, mobile phones have good wireless connections, work fast and can be used for several different needs.[77] With a modern phone, you can take photos, use the internet, read and write e-mails and also pay your groceries in a shop.

The development in technology, especially in communications and information technology, has lead to insecurity in protection of privacy and personal data.[78] The development of computers and mobile phones has made it possible for the social media applications and other networks to develop rapidly.[79] Social media applications almost always require some personal information about the user before he or she can use the application, and this is one of the reasons, why the

[72] *Bygrave* 2002, p. 93.
[73] *Ibid.*
[74] *Caloyannides* 2004, p. 301.
[75] *Bygrave* 2002, p. 93.
[76] *Bygrave* 2002, p. 94.
[77] *Ibid.*
[78] *Psychogiopoulou* 2017, p. 32.
[79] *Ibid.*

personal data protection is an important topic for legal discussion in international and national level[80].

These developments have changed the way people socialize and talk to each other.[81] Instead of going to a restaurant to meet a friend, people stay at home and chat with a friend in Facebook or in other networks.[82] This has also made the law enforcements to develop their surveillance devices that will adapt better to the modern way of living.[83]

Even though the modern world is highly technological and computerized, it is important to also highlight the humane sides in the world.[84] Personal data is not just letters and number and, personal data plays an important role in data subject's life. People, who use for instance mobile phones and social media applications, should have the right to be sure that their personal data is being handled carefully.[85]

The question of who can collect, process and store personal data of individuals raises concern among individuals[86] and, also the fact that not only the personal data subject has rights, but also the counterpart has rights. For instance, both the internet users and controllers of the internet sites have fundamental rights and they might often collide with fundamental rights of the internet users.[87] Internet users have fundamental right to have control on their personal data, while the internet controllers have a fundamental right to use the data as needed in order to maintain the economic development and welfare.[88]

Retailers collect information about their customers in the internet by requiring personal information before the customer can use their website.[89] These websites

[80] *Heisenberg* 2005, p. 162.
[81] *Newman* 2008, p. 125.
[82] *Ibid.*
[83] *Ibid.*
[84] *Selmer* 1990, p. 27.
[85] *Ibid.*
[86] *Psychogiopoulou* 2017, p. 32.
[87] *Antikainen* 2014, p. 1.
[88] *Ibid.*
[89] *Caloyannides* 2004, p. 301.

also track the customers behavior while using the website and collect this tracked data.[90] This helps the retailers to target advertisements to the right audience.[91]

In addition to commercial fairs, personal data can be used to other means as well with the help of technology. For instance, there is a legal process in the United States, which is technical and works in the Internet, and is very abusive by its nature.[92] This legal process enables, for instance, a big retail company to figure out and identify an individual, who has given bad feedback anonymously to the company through the internet.[93] To get this information, these companies subpoena the internet data controllers, which forces them to reveal the data they have collected.[94] This identification process seems unfair for the data subject and also for the data controllers, who have been subpoenaed.[95]

With technological developments, lot of the data, for instance medical data in the hospitals and legal evidence in a criminal case, have moved from the files in the cabinet to the computer and internet files. Again, there is risk that, for instance, evidence from a criminal case spreads all over and is abused[96], which makes the work of law enforcements' harder and might give wrong information about the investigation to the people. To prevent this, there is a group of knowledge management professionals, who work against the spreading of data and, also, for putting the spread data back together.[97]

Even though technological developments bring some challenges to work of law enforcements, they have also brought some new equipment and ways to control and fight against terrorism and crime. However, these ways and equipment aren't always in accordance with the personal data protection regulations. The balance between national security and the personal data protection is challenging in this world, where personal data protection is more and more important, but where terrorist and criminal acts happen daily.

---

[90] *Caloyannides* 2004, p. 301.
[91] *Ibid.*
[92] *Caloyannides* 2004, p. 303.
[93] *Ibid.*
[94] *Ibid.*
[95] *Ibid.*
[96] *Caloyannides* 2004, p. 316.
[97] *Ibid.*

2.3. Terrorism and crime

In 2013, two homemade bombs detonated near the finish line of Boston marathon.[98] Faces of the bombers were caught on camera which helped to identify and catch the two bombers.[99] The number of cameras have increased since the incident which, according to Kade Crockford, is problematic in the light of privacy and personal data protection.[100] Crockford says that surveillance in bigger events is understandable, but the installation of cameras "that enable law enforcement to track individual people from the moment that we leave our homes in the morning until the moment we return at night, seeing basically everywhere we went and everything that we did" does trigger privacy issues.[101]

In addition to the Boston bombings, 9/11 attacks in New York and the attacks in Europe, for instance Madrid, London and Paris, prove that these kind of terroristic attacks may take place quite unexpectedly.[102] This thread has been recognized in the Western countries, which can be seen, for instance, in Europe and in its legal and cultural changes.[103] An example of these changes are the attempts, made by the national security agencies, to get authorization for wider monitoring of people by the means of catching terrorists and criminals before they manage to do their act of crime.[104] There is also a cross border co-operation between nations when they share the monitored or collected data when they are trying to find or catch an international terrorist or criminal.[105]

As has been discovered before, privacy protection and data protection do not always prevail when they collide with other rights.[106] For instance, personal data protection might be restricted for the means of national security.[107] Cameras in the streets and stores record your every move and even your face, and the recorded

[98] *NPR* https://www.npr.org/2015/04/17/400164221/boston-marathon-surveillance-raises-privacy-concerns-long-after-bombing?t=1553158085133, read 21.3.2019.
[99] *Ibid.*
[100] *Ibid.*
[101] *Ibid.*
[102] *Colonna* 2016, p. 198.
[103] *Ibid.*
[104] *Newman* 2008, p. 125.
[105] *Ibid.*
[106] *Kremer* 2017, p. 118.
[107] *Ibid.*

data is collected and stored. This interferes clearly with personal data protection and also with the right to private life.[108] These restrictions are acceptable to the point the restrictions are necessary.[109] It is the responsibility of the agencies, who make these restrictions, to make sure the right to personal data protection isn't restricted too much in the name of national security.[110] That is why the agencies need to assess the stored data from different angles and perspectives before they can publish this kind of data in the means getting public help in catching terrorists and criminals.[111] For instance, it is required to assess whether it is actually required to publish the data and whether the publication causes more damage than advantages.[112]

The principles that concern, for instance, personal data protection restrictions are stated in the international human rights law and in the International Covenant on Civil and Political Rights (ICCPR).[113] These principles are, according to the ICCPR, the principle of legality, necessity and proportionality and they need to be considered when making limitations to personal data protection in the means of national security.[114] A good example of these principles in action is from a criminal case, where collected evidence, for instance telephone records, can only be stored until the end of the investigations and when the investigations have been finished, the stored data must be deleted.[115] In other words, to the point they are necessary.[116]

The European Court of Human Rights (ECtHR) has evaluated the acceptable interference in personal data protection in the means of national security.[117] In its memo from 1978, the ECtHR recognized the thread of terrorism and stated that; "the existence of some legislation granting powers of secret surveillance over the mail and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention

[108] *Boehm* 2012, p. 36.
[109] *Kremer* 2017, p. 118.
[110] *Ibid.*
[111] *Boehm* 2012, p. 40.
[112] *Ibid.*
[113] *Kremer* 2017, p. 123.
[114] *Ibid.*
[115] *Boehm* 2012, p. 64.
[116] *Ibid.*
[117] *Boehm* 2012, p. 63.

of disorder or crime".[118] The statement is quite old, yet it is still accurate.[119] In this data protection age, the fight against terrorism and crime with the help of data collection and surveillance measures is acceptable.[120] The EU member states have been granted with wide possibilities of implementing data protection legislations in counter terrorism measures.[121]

Europe and the EU has taken an important role in the development of international data protection regulations. This might have been one of the reasons for the conflicts between the US and Europe.[122] These conflicts of course affected negatively on the co-operation against international terrorism and crime.[123] The conflict originated from the US's decision to collect detailed airline data about customers, who flew from Europe to the US.[124] This decision conflicted with the EU privacy and data protection legislations.[125] This conflict has been settled with the help of the allies of North Atlantic Treaty Organization (NATO)[126], yet these sort of conflicts might appear in the future as well.

Co-operation is the key for the international counterterrorism, but the developed technology is just as needed in this kind of co-operation. One good technological instrument is data mining.[127] Data mining is an application, which assesses the data it's given, and is able to search for the previously unknown features of the data.[128] In the fight against terrorism and crime, data mining is used for predicting upcoming terrorist and criminal actions and also to learn more carefully about criminal behaviour.[129]

In the end, from international co-operation between nations and data mining, the personal data protection issues always come down to the people. As I stated already before, people don't mind giving up and storing their personal information

[118] *Boehm* 2012, p. 63.
[119] *Ibid.*
[120] *Ibid.*
[121] *Ibid.*
[122] *Newman* 2008, p. 5.
[123] *Ibid.*
[124] *Ibid.*
[125] *Ibid.*
[126] *Ibid.*
[127] *Colonna* 2016, p. 32.
[128] *Ibid.*
[129] *Colonna* 2016, p. 198.

in the internet.[130] However, it has been said that when the personal data is being collected and stored by the state, people seem more concerned about the protection of their personal data.[131] Michael Friedewald, Marc van Lieshout, Sven Rung and Merel Ooms have researched these attitudes and the results do not speak for such a strict attitude as stated in the last sentence.[132] According to these research results, people trust the government institutes that have collected and stored their personal data.[133] In addition, in a colliding situation, people support more the practices that are needed for national security than for individual privacy and data security.[134]

Internationalism, technology, terrorism and crime are all quite clear threads for personal data protection. However, the international and national economy forms also one serious thread to personal data protection[135] about which I shall tell more about in the next chapter.

2.4. Economy

The relationship between data protection and economy is two folded.[136] While personal data is being abused in the name of economic development, at the same time breaches and violations of personal data causes enormous economic losses world widely.[137] For instance, solely in the United States the economic losses caused by data breaches, such as identity thefts, are over 50 billion dollars annually.[138] In a way, data protection and economy challenge each other.

Personal data regulations play an important role in resolving international disputes that concern economic issues.[139] However, at this point of this thesis, it is

[130] *Friedewald – Lieshout – Rung – Ooms* 2016, p. 56.
[131] *Ibid.*
[132] *Ibid.*
[133] *Ibid.*
[134] *Ibid.*
[135] *Kremer* 2017, p. 104.
[136] *Newman* 2008, p. 1.
[137] *Ibid.*
[138] *Ibid.*
[139] *Newman* 2008, p. 5.

quite clear that there are very different approaches and regulations to data privacy and to data protection all around the world, which might be challenging for these kinds of disputes. Some countries, such as the United States, have systems where the economic development and efficiency has privilege over individual and consumer data privacy, whereas in some other countries, for instance in Europe, the situation is reversed.[140] This has caused conflicts between countries, which has affected to the economic growth and co-operation.[141] However, despite all this, the European type of rules and regulations on data privacy and data protection, such as the EU data privacy directive from 1995, have spread widely around the world and have shaped the economic development world widely.[142]

International organizations have also given their own views to the relationship between personal data protection and economic welfare. One significant set of guidelines has been written by the international organization called the Organization for Economic Co-operation and Development (OECD).[143] The OECD's goal and mission is to give international guidelines that would be helpful and useful for economic situations all around the world.[144] As I said, the OECD has given guidelines for data protection in economic affairs[145] and I will go through these guidelines later on in this thesis in chapter 4.2.2.

Even though the European model is the controlling model internationally, it cannot prevent the transferring of data in business affairs.[146] It even has been said that in business affairs it is impossible to attain from giving your personal information to someone.[147] You cannot enter a business deal or purchase something from the internet without giving your personal information.[148] However, the idea in EU personal data protection regulations is not the total prevention of personal data collection and storing, but the controlling of data collection and also the preventing

[140] *Newman* 2008, p. 2.
[141] *Ibid.*
[142] *Newman* 2008, p. 2-3.
[143] *Tzanou* 2017, p. 15.
[144] *Kosta* 2013, p. 26-27.
[145] *Tzanou* 2017, p. 14.
[146] *Newton* 2014, p. 164-165.
[147] *Ibid.*
[148] *Ibid.*

of personal data abuses.[149] For instance, the online data collection in the means of marketing falls under the scope of the EU personal data protection regulations.[150]

The personal data protection regulations actually cannot be too strict, if we want to continue with the development of international trade and economy.[151] It has been said that the blocking of the free flow of data complicates the international economy affairs.[152] Antti Antikainen has said well in his thesis that "a too strict privacy regulation could block this area of economic activity, which would be against the fundamental rights of the data controllers as legal persons also causing welfare losses to the whole community".[153] This is a common practice and ideology in international trade and that is why international companies can rely on the free flow of data within their business affairs.[154]

The principle of the free flow of data enables companies to create accurate advertisements to the right audience.[155] The more apt the advertisement is, the more appealing it is to the customer and leads into a business deal.[156] Internet websites and social networks collect data about their users and create sort of commercial profiles, which help the websites and social networks to direct even better right advertisements to the right audience.[157] To do this kind of an advanced profile of a website or social network user for commercial means, it requires a lot of personal data about users.[158] For this reason, many of the social networks have clause in their conditions which enables the network provider, such as Facebook, to use almost any of the data a user has stored in the network and in his or hers own profile.[159] A straight quote from the conditions of Facebook is as follows; "For content that is covered by intellectual property rights, like photos and videos you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook. This

[149] *Léonard – Skouma* 2015, p. 47.
[150] *Ibid.*
[151] *Newman* 2008, p. 5.
[152] *Ibid.*
[153] *Antikainen* 2014, p. 1.
[154] *Newman* 2008, p. 5.
[155] *Graef* 2016, p. 125.
[156] *Ibid.*
[157] *Ibid.*
[158] *Graef* 2016, p. 135.
[159] *Ibid*.

IP license ends when you delete your IP content or your account unless your content has been shared with others and they have not deleted it."[160]

The marketing and advertising started already in the 1990s and has developed ever since.[161] Already in the 1990s, the internet, together with the personal data that has been collected from websites and other networks, has been seen as good platform for marketing and advertising.[162] During the recent years, many big companies, such as Microsoft, Yahoo and Google, have concentrated on advertising in the internet and have invested tremendously in this.[163] So instead of getting an advertisement in paper in your mailbox, you will more likely get same advertisement on your Facebook wall, but only if you belong to the targeted audience.

It is clear that data and personal data is being used as a tool for economic development and growth. However, nowadays personal data is being used as a new asset[164] and it has been described as a 'new currency'.[165] Some companies already accept the personal data of their customers as a payment for the purchased good or service.[166] A good example of this is the US telecommunications company AT&T's practice to give monthly discount for customers, who let the AT&T to track them online.[167]

Considering all the above written facts about using personal data as a currency and as a tool for marketing, it is not a surprise that there is a lot of discussion and debate about online personal data protection. The discussion has, however, concentrated on questions about how and with what manners has the data been collected.[168] The usage of such data hasn't raised as much discussion nor debate.[169] Many of the online advertisers state that their actions in data collection have only positive outcomes when the data subjects get advertisements that might actually

[160] *Graef* 2016, p. 135.
[161] *Chester* 2012, p. 56.
[162] *Ibid.*
[163] *Ibid.*
[164] *Graef* 2016, p. 126.
[165] *Ibid.*
[166] *Ibid.*
[167] *Ibid.*
[168] *Chester* 2012, p. 63-64.
[169] *Ibid.*

interest them and so their data collection manners do not cause any harm to anyone.[170]

Despite this 'promise' made by the above-mentioned data collectors, data subjects have the right to have their collected data of being destructed right after the data is no longer needed for the purpose they were originally collected.[171] The destruction of data might be the most challenging phase in the timeline of processing personal data because, as I have stated before, once you store some personal data in the internet, it might be impossible to delete and destruct this data from everywhere in the Internet.[172]

Here I have now presented some of the modern threads and challenges that personal data protection faces daily. As can be seen, these different challenges, such as technology and economy, are tightly connected to each other and when there is a challenge with one of these mentioned above, there is a significant chance that some other challenge occurs at the same time. The best way to explain this concretely is probably to go through some relevant legal cases, but before I shall go through some cases, I will tell about the current EU data protection legislations and regulations.

[170] *Chester* 2012, p. 63-64.
[171] *Léonard – Skouma* 2015, p. 49.
[172] *Ibid.*

3. Protection of personal data in Europe and in European Union law

3.1. Fundamental rights and human rights

3.1.1. The two statutes: European Convention on Human Rights (ECHR) and The Charter of Fundamental Rights of the European Union (CFREU)

Fundamental rights and human rights are internationally proclaimed rights of individuals and they have been developing continuously for decades.[173] From the international perspective, there are various documentations about fundamental rights and human rights.[174] In the EU level, there are two important and relevant documents about the fundamental and human rights. The first one is the Convention for the Protection of Human Rights and Fundamental Freedoms, in other words the European Convention on Human Rights (ECHR), which came into force in 1953.[175] Its ultimate purpose was to make the fundamental rights stated in the Universal Declaration of Human Rights (UDHR) legally binding and to protect human rights and fundamental freedoms of the individuals.[176] The European Court of Human Rights (ECtHR) was then established to work as the court, which processes cases that concerns the violations of the ECHR rights.[177] It has been amended many times after it came into force.[178]

The second one is the Charter of Fundamental Rights of the European Union (CFREU) and the first version of it came into force in 2000.[179] The amended version came into force at the same time with the Treaty of Lisbon in 2009.[180] The CFREU wasn't recognized as legally binding charter when it first came into force in

[173] *Hakapää* 2010, p. 165.
[174] *European Commission,* https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_fi#what-it-covers, read 22.3.2018.
[175] *Ibid.*
[176] *Kosta* 2013, p. 17.
[177] *Ibid.*
[178] *Ibid.*
[179] *Ibid.*
[180] *Ibid.*

2000, but when the Lisbon Treaty was adopted, also the CFREU got its force as a legally binding charter.[181] In the first pages of the CFREU, it has been declared that it reinforces the international constitutional regulations that are applied in EU, in its organizations and in its member states.[182] In addition, in the same first pages it has been said that the mission of CFREU is to, again, reinforce the status of fundamental rights, when they are challenged by the modern threads and challenges,[183] which have been mentioned in the previous chapters of this thesis.

Both the ECHR and the CFREU have strengthened the status of personal data protection and specially as a fundamental right.[184] However, there is a clear difference between the statuses when considering the personal data protection and, also, the protection of privacy.

According to the ECHR, the right to respect for private and family life has been enacted in Article 8. There is no clear definition of the area of interpretation of this Article, but according to the legal praxis of the European Court of Human Rights (ECtHR) the protection of personal data is being judged under Article 8 of ECHR.[185] In the legal praxis of ECtHR it has been stated that "the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life" and that "the domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article".[186] It can be concluded from this that, according to the ECHR and ECtHR, the protection of personal data is indeed part of the fundamental right to privacy.

The CFREU has a different kind of approach to data protection and privacy protection, and it has created a 'new' fundamental right[187], which has been lead from the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[188] In Article 7

[181] *Colonna* 2016, p. 126.
[182] *Gonzaléz Fuster* 2014, p. 193.
[183] *Ibid.*
[184] *Boehm* 2012, p. 123.
[185] *Psychogiopoulou* 2017, p. 33.
[186] *S. and Marper v the UK* App nos 30562/04 and 20566/04 (ECHR, 4 December 2008), para. 103.
[187] *Tzanou* 2017, p. 20.
[188] *Neuvonen – Rautiainen* 2015, p. 45.

of the CFREU is the fundamental right to respect for private life. In Article 8 is a separate right for the protection of personal data. This differs from the ECHR, because the ECHR doesn't have an independent Article for personal data protection.

The ECHR is from the 1950s and the CFREU is from the 21st century, and these different eras can be seen when their Articles are being compared.[189] As stated above, the CFREU has two separate Articles for the protection of one's privacy and for the protection of personal data when the ECHR has only an Article for the protection of private life.[190] The CFREUs model obviously recognizes the personal data protection as an independent fundamental right.[191] The fundamental rights to respect for private life and personal data protection have been regulated from different kind of perspectives.[192] The fundamental right for the respect for private life is a negative right; it's purpose is to prevent the breaches of private life instead of ruling specific actions that ought to be done for the protection of private life.[193] The fundamental right to data protection, however, is a positive right.[194] The fundamental right to personal data protection hasn't been enacted only for the prevention of data breaches.[195] Instead, it declares the rules that what can and cannot be done with someone's personal data.[196]

The EU legislation plays an important role in the developing of the fundamental rights and it gives the leading example on the personal data protection's status as a fundamental right.[197] Internationally the CFREU Article 8 is the first specific fundamental right for personal data protection.[198] It has even been said that now, that personal data protection has its own Article in CFREU, it has the status of an independent fundamental right, at least within the EU jurisdiction.[199]

[189] *Rodotà* 2009, p. 79-80.
[190] *Ibid.*
[191] *Ibid.*
[192] *Ibid.*
[193] *Ibid.*
[194] *Ibid.*
[195] *Ibid.*
[196] *Ibid.*
[197] *Tzanou* 2017, p. 16.
[198] *Tzanou* 2017, p. 18.
[199] *Ibid.*

Despite the way personal data has been protected, the need for personal data protection has been recognized in EU and all over the world as well.[200] Data subjects themselves and international and national authorities are responsible for the personal data protection.[201] It seems that especially in EU the situation is good; there are two significant regulations that protect the privacy and the personal data of the people. The ECHR and the CFREU support each other and the rights concerning the same issues have similar meanings.[202] In other words, they are both applicable in similar situations.[203]

However, the status of personal data protection as a fundamental right and theories concerning this status still remains unanswered. In the next chapter, I shall look closer to this issue in the light of the ECHR and the CFREU.

3.1.2. Fundamental and human right status theories

Fundamental and human rights are rights that have an important status in legal sphere.[204] These rights have once been granted to all the people and cannot be restricted without good enough reason.[205] The terminological difference between fundamental and human right comes from different cultures and languages.[206] However, the content of these terms doesn't differ from each other that much and that is why, as I stated above, I will use them as synonyms.

As has been noted in this thesis before, there are differences between the existing regulations on the fundamental right to privacy and personal data protection in Europe. There are also differences in the interpretation of these fundamental rights. As a repetition from the previous chapter, the CFREU has separate articles

[200] *Blume* 2001, p. 9.
[201] *Rodotà* 2009, p. 79-80.
[202] *European Commission,* https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_fi#what-it-covers, read 22.3.2018.
[203] *Ibid.*
[204] *Gonzaléz Fuster* 2014, p. 164-165.
[205] *Ibid.*
[206] *Ibid.*

for fundamental right to privacy, Article 7, and for fundamental right to personal data protection, Article 8, when the ECHR has only the protection for private life in Article 8. The Court of Justice of the European Union (CJEU) has mainly interpreted the CFREU while judging cases concerning privacy or personal data protection issues, and the legal praxis seem to have strengthen the protection of the rights in Articles 7 and 8.[207] One difference between these two regulations is also the fact that the ECHR is a slight more general by its nature and the CFREU brings the fundamental rights closer and more clearly to the people.[208]

Despite the improved statuses of fundamental rights to personal data protection and the right to privacy, the difference or distinction between these two rights is not quite clear.[209] For some time, the CJEU wasn't quite certain about how it was supposed to interpret the Articles 7 and 8 of the CFREU.[210] However, in 2014 and 2015 the approach to these Articles changed.[211] There were few cases, such as case C-293/12 Digital Rights Ireland[212] which I will go through more precisely later, were the personal data protection was seen and interpreted as an independent fundamental right.[213] In addition, it has been said that the fundamental right to data protection was somewhat created by the CJEU in a case called *Promusicae.*[214] The CJEU, however, did not make any distinctions between data protection and privacy in this case.[215] I shall go through the *Promusicae* case, and also the above mentioned case about Digital Rights Ireland, more carefully in chapter 3.3.

In addition to the development in the EU jurisprudence, legal scholars have theories about fundamental and human rights and also about the fundamental status of personal data protection. According to Maria Tzanous' theory, in order for the data protection could be seen as an independent fundamental right, it needs to be separated from the supportive legislations through which data protection is seen as a fundamental right.[216] In other words, it is necessary to assess the

[207] *Brkan* 2017, p. 10.
[208] *Ibid.*
[209] *Brkan* 2017, p. 11.
[210] *Tzanou* 2017, p. 58.
[211] *Ibid.*
[212] *Ibid.*
[213] *Tzanou* 2017, p. 62-63.
[214] *Ibid.*
[215] *Brkan* 2017, p. 11.
[216] *Tzanou* 2017, p. 38.

autonomous fundamental value of data protection.[217] According to the EU constitutional law it is required that in order to see a right as a fundamental right, it needs to have an autonomous status.[218] Since the personal data protection is listed in the CFREU, it is compulsory that data protection is an autonomous fundamental right.[219] So the starting point for Tzanous theory is that data protection cannot be seen as an independent fundamental right, if it doesn't meet with the autonomous requirement the EU constitutional law has set for fundamental rights.[220]

In her theory, Tzanou has assessed how data protection functions by itself and whether it needs to be supported by the fundamental right to privacy or other legislation[221] and, despite its close connection with privacy and other legislation and its unclear content,[222] Tzanou has said that "there is no reason why data protection cannot operate as a bona fide fundamental right and have a normative significance."[223]

The two scholars, Paul De Hert and Serge Gutwirth, have the same outcome as Tzanou about the status of data protection yet they have a different kind of theory and approach to fundamental rights.[224] This theory is critized by Tzanou.[225] De Hert and Gutwirth aim to reason the fundamentality of data protection and to reason its status as a fundamental right with the help of the fundamental right to privacy.[226] Tzanou thinks that the two scholars fail in this, because their theory does not merely focus on data protection and the added value of data protection is demonstrated through its distinction from privacy.[227] When the importance of data protection is explained by its distinction to privacy, it is not sufficient enough and does not explain its constitutional entrenchment.[228]

---

[217] *Tzanou* 2017, p. 38.
[218] *Tzanou* 2017, p. 38-39.
[219] *Ibid.*
[220] *Tzanou* 2017, p. 36.
[221] *Ibid.*
[222] *Tzanou* 2017, p. 247.
[223] *Tzanou* 2017, p. 250.
[224] *Tzanou* 2017, p. 33.
[225] *Ibid.*
[226] *Ibid.*
[227] *Ibid.*
[228] *Ibid.*

It strongly seems like in EU jurisprudence the personal data protection has an independent fundamental status. Even though the fundamental status of a right depends on the specific rights' autonomy, the supportive, in other words secondary, legislation needs to be in accordance with and support the fundamental and human rights. That is why I will go through the relevant secondary legislation starting with the directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which is at this date no longer in force.

3.2. The European Union regulation on data protection

3.2.1. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

The EU and especially the EU Commission are actively developing the EU legal systems and monitoring the modern changes that occur around the world.[229] This monitoring helps the EU to keep its regulations and legislations up to date and applicable in the modern world.[230] In this developing and monitoring process the personal data protection and privacy have an important role,[231] which is probably one reason for the comprehensive data protection and privacy regulations in the EU.

The preamble of the directive 95/46/EC states, that the directive was enacted on the 24th of October in 1995 and was the previous regulation 'on the protection of individuals with the regard to the processing of personal data and on the free movement of such data'. It was overruled by the General Data Protection Regulation (GDPR), which will be presented in chapter 3.2.2. Even though this directive isn't no longer in force, it seems to me that it was the first significant EU

[229] *Boehm* 2012, p. 9.
[230] *Ibid.*
[231] *Ibid.*

directive about personal data protection, and it was the springboard for the new GDPR, which is why it is important to explore the directive 95/46/EC too.

The directive 95/46/EC, which I will refer to as the data protection directive from now on, was regulated for data protection and data privacy.[232] There were two main goals for the data protection directive.[233] The first goal was to harmonize the EU member states regulations on data protection which would ensure the free flow of data between member states.[234] The second goal was to inform the member states that the EU is willing to invest in personal data protection.[235]

The data protection directive has 34 Articles that cover, for instance, personal data transfers to countries outside the EU, confidentiality and security of personal data in processing of such data and the data subject's rights to have access to his or her data. The data protection directive has Articles that support the free flow of data in the name of economy and also Articles that protect fundamental right to data protection and privacy.[236] The data protection directive, however, doesn't have Articles for data breaches.[237] According to the data protection directive, the data controllers do not have a responsibility to tell about data breaches to the investigative party, called the Data Protection Authority (DPA), who investigate data breaches that they are aware of.[238] This has been taken into account in the new GDPR and the data controllers have the responsibility to inform the Data Protection Authority and the data subject in question about data breaches.[239]

In addition to the EU member states, the data protection directive has had effect in other countries too.[240] Countries that have, for instance, economic contacts with a EU member state and vice versa were influenced by the data protection directive.[241] Since 2004, the derogations in data protection directive's Article 26 were applied to many of the transfers from an EU member state to states outside of

[232] *Newman* 2008, p. 74.
[233] *Ibid*.
[234] *Ibid.*
[235] *Ibid*
[236] *Lynskey* 2013, p. 59.
[237] *Wong* 2013, p. 25.
[238] *Ibid.*
[239] *Ibid.*
[240] *Heisenberg* 2005, p. 104.
[241] *Ibid.*

the EU.[242] In the Article 26 it has been stated, among other things, that the data subjects consent is required when his or her data is being transferred to a country, where the data protection isn't on the same legislative level as in the EU, and that the transfer of data must be necessary for the "conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party" or "the transfer is necessary in order to protect the vital interests of the data subject".

According to this same Article 26, the EU member states were supposed to inform the EU Commission about data transfers to countries that do not have adequate level of data protection.[243] This adequate level of data protection has been stated in the previous Article, Article 25. However, the Commission hasn't received as many reports about these transfers as could have been anticipated.[244] The Commission has suspected that many illegal data transfers might have happened since 1998, when the applying of the data protection directive started.[245] This allegation cannot be confirmed because of the lack of enforcement actions in this matter.[246]

As I wrote before, the data protection directive is no longer in force and has been replaced with the new regulation, the GDPR. This is part of the EU personal data protection change that the Commission introduced already in 2012.[247] The Commission signaled about changes in fundamental rights and also in the approach to personal data protection, privacy and their relationship.[248] The Commission flashed the right to the personal data protection as a distinctive right from the right to privacy.[249] The EU Commission also introduced a new perspective to the right to privacy and to the right to personal data protection, and this perspective was the right to be forgotten.[250] All of these were important factors when the new GDPR was regulated, enacted and later put into force.

---

[242] *Heisenberg* 2005, p. 113.
[243] *Heisenberg* 2005, p. 114.
[244] *Ibid*.
[245] *Ibid*.
[246] *Ibid*.
[247] *Gonzaléz Fuster* 2014, p. 248.
[248] *Ibid*.
[249] *Ibid*.
[250] *Ibid.*

3.2.2. The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) was enacted in the 26th of April in 2016 and it has been applied ever since the 25th of May in 2018. According to the preamble of the GDPR, its purpose is to ensure the protection of personal data when its being gathered, processed and registered. The GDPR is in many ways a lot wider than its preceding statute, the data protection directive. The GDPR has 99 Articles, which have been divided into the following 11 Chapters; General provisions, Principles, Rights of the data subject, Controller and processor, Transfers of personal data to third countries or international organisations, Independent supervisory authorities, Cooperation and consistency, Remedies, liability and penalties, Provisions relating to specific processing situations, Delegated acts and implementing acts and Final provisions.

The GDPR brought some key changes to the EU privacy and data protection regulation.[251] First, the GDPR changed the territorial scope of the EU data protection regulation.[252] The GDPR applies also to those data collectors and processors who might not be in the EU area, but who collect and process data that belongs to EU residents.[253] Second change concerns the penalties and according to the GDPR those who violate or breach the GDPR, can be fined.[254] The third change requires the data collectors and processers to make their customer conditions and terms of use clear, where the consent for the usage of customers data can be seen clearly and distinguished from the other terms.[255]

The final and probably the biggest changes concern the data subject and his or her rights.[256] According to the GDPR, the data subject has the right to know whether his or her data has been breached, has the right to access to his or her data and has the right to be forgotten.[257] In addition, the data subject has the right to trust that the data controllers and processers have secure platforms for processing the

[251] *GDPR,* https://eugdpr.org/the-regulation/, read 21.5.2019.
[252] *Ibid.*
[253] *Ibid.*
[254] *Ibid.*
[255] *Ibid.*
[256] *Ibid.*
[257] *Ibid.*

data.[258] Also, the data subjects have right to trust that the data protection supervisors make sure the data protection standards are met in controlling and processing of data.[259]

These improvements seem good and hopefully these will work in real life too, but before this is possible, some of the terms need to be clarified. Those terms are 'processing' and 'personal data', because they are central in data protection issues and in regulations relating to it.[260] That is why it is important to give as clear as possible definitions to these words.[261] Processing of data is quite broad by its definition.[262] It is, for instance, collection, use and deleting of data, and any other performance done with data.[263] The personal data, for one, is any data that a person can be linked to or identified from.[264]

In the preamble of the GDPR it has been written that the GDPR "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".[265] As can be seen from this, and also from other sections of the regulation, the GDPR sees the personal data protection as a fundamental right. However, in GDPR it has also been stated that it is not an absolute right. According to GDPR, the protection of personal data "must be considered in relation to its function in society and be balanced against other fundamental rights". This is of course quite an obvious statement. Fundamental and human rights must be interpreted and applied in a way, which does not make other fundamental and human rights null and void. This balancing between different fundamental rights can be best presented by the following cases. The GDPR is such a new regulation that there aren't really any cases where the GDPR would have been applied, which is why in these following cases we can see how the data protection directive, the CFREU and the ECHR have been applied in legal praxis.

---

[258] *GDPR,* https://eugdpr.org/the-regulation/, read 21.5.2019.
[259] *Ibid.*
[260] *Tzanou* 2017, p. 12.
[261] *Ibid.*
[262] *Tzanou* 2017, p. 12 – 13.
[263] *Ibid.*
[264] *Tzanou* 2017, p. 13.
[265] *Tzanou* 2017, p. 12.

3.3. Case studies

In the EU there are two Courts that are relevant in this thesis. The first one is the European Court of Human Rights (ECtHR), which applies primarily the ECHR, and the second one is the Court of Justice of the European Union (CJEU), which applies primarily the CFREU.

The ECtHR is an organ for the protection of human rights and, also, an EU organ for providing guidelines concerning human rights.[266] The ECtHR jurisdiction has successfully brought many of the modern technological developments, such as computers, internet and video-surveillance, under the scope of ECHR Article 8, the right to respect for private and family life.[267] From the ECtHR jurisdiction it can be seen which data categories have already been protected and which definitely are seen as belonging in the scope of the interpretation of the ECHR Article 8.[268] At least the following categories belong in this scope; telecommunication data, audio or video material containing personal information, photos, medical data, DNA samples, fingerprints and personal data on the internet.[269]

The relevant ECtHR cases concern mostly the balance between different rights or interference of a fundamental right in the name of national security and crime prevention.[270] Throughout the years, the ECtHR has judged many cases where the relationship and precedence between the ECHR Article 8 and other ECHR rights have been assessed.[271]

The ECtHR has more and more highlighted the importance of personal data protection and its profound connection to the right to respect for private and family life.[272] Because of this close connection, in the previous ECtHR case law the right to data protection was quite often applied through or together with the right to respect for private and family life.[273] However, nowadays the ECtHR seems to

[266] *De Hert – Gutwirth* 2009, p. 15-16.
[267] *Ibid.*
[268] *Boehm* 2012, p. 31-32.
[269] *Ibid.*
[270] *Psychogiopoulou* 2017, p. 49-50.
[271] *Psychogiopoulou* 2017, p. 59.
[272] *Boehm* 2012, p. 25.
[273] *Ibid.*

have taken a different approach to data protection and interprets or applies it as an independent right.[274]

The CJEU case law hasn't been as progressive as the ECtHR case law when considering the independence of personal data protection.[275] The CJEU jurisdiction in data protection issues has made it clear that the CJEU sees the fundamental right to personal data protection as a part of the right to privacy and that it cannot function independently.[276] At least this was the initial approach when the CFREU became legally binding and now its seems that the CJEU jurisdiction has developed from this.[277]

These were some of the general insights given based on the legal praxis of the ECtHR and CJEU. The following relevant and significant cases for this thesis, that have been judged in CJEU and ECtHR, hopefully open these insights even better.

Court of Justice of the European Union

1) Case C-275/06 *Promusicae* [2008] ECLI:EU:2008:54

   In this case, the parties were the Producters de Musica de España (Promusicae), who produce and publish music videos, and Telefónica, which is a company providing 'internet access services'. The Promusicae asked the Telefónica to give it the personal data records of certain customers, whom it suspected to have breached the intellectual property rights (IPR) of its work. Telefónica refused to give this information and so the case was taken into the national court.

   The national court assessed the case and then asked for preliminary ruling from the CJEU. The national court asked whether it was supposed to grant the Promusicae the information it requested in order to secure the

[274] *Boehm* 2012, p. 28.
[275] *Tzanou* 2017, p. 54.
[276] *Tzanou* 2017, p. 55.
[277] *Ibid.*

fundamental right to IPR rights. The CJEU didn't give a straightforward answer what to do and instead reminded that the EU member states were supposed to maintain the balance between different fundamental rights, like in this case between IPR rights and right to data protection, and evaluate the balance separately in every case.

This case wasn't a breakthrough for the fundamental right to data protection.[278] The personal data protection was acknowledged, but didn't have a remarkable impact as in independent fundamental right.[279] The CJEU's wording that "the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other", without making any distinctive mention about the data protection itself, gives an image that the data protection is seen as part of the right to private life in this case.[280]

2) Case C-207/16 *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788

In this case the CJEU gave a preliminary ruling about the processing of personal data and the security of telecommunications. Mr. Hernandez Sierra was robbed, and his wallet and phone got stolen. Mr. Sierra reported this to the police, who started to investigate the incident. The police requested from the telecommunications services for the telephone numbers and personal data connected to the stolen phone from a certain timeline in order to catch the thieves. The request was denied, because it was against personal data protection regulations and because it was thought that it wouldn't help to identify nor to catch the thieves. This decision was based in the ideology that these kinds of requests were accepted only when a much more serious offence was in question.

[278] *Gonzaléz Fuster* 2014, p. 227.
[279] *Ibid.*
[280] *Ibid.*

The national court of Spain, however, asked for the CJEU to give a preliminary ruling on what would be the adequate interference of the Articles 7 and 8 of the CFREU in this kind of cases. While balancing between personal data protection and criminal justice, the national court wondered whether it was enough to just determine the seriousness of the offence or whether it was also needed to judge the harmfulness of the offence to an individual.

The CJEU ruled that the seriousness of the offence needs to be judged, as well as the seriousness of the interference of the fundamental rights. About this case, the CJEU ruled that the police could have been granted with the data it requested. The CJEU saw that it wouldn't have been a serious interference of Articles 7 and 8 if the data had been granted. In its reasoning, the CJEU highlighted that this sort of interference is not "sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime".

3) Joined Cases C-293/12 *Digital Rights Ireland Ltd* and C-594/12 *Kärntner Landesregierung* [2014] ECLI:EU:C:2014:238

In these cases the question and the CJEU preliminary ruling concerned the validity of 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.

In these cases, the most interesting and relevant part is CJEUs reasoning about the validity of the Directive 2006/24/EC. The CJEU evaluated the validity of the directive in the light of CFREU Articles 7 and 8. Based on this evaluation, the CJEU stated that the directive is indeed invalid. The CJEU ruled that the directive interfered with the two fundamental rights and by

passed the principle of proportionality. For instance, the directive did not guarantee good enough protection for the collected data, did not outline the territorial area, where the data must be stored, and did not outline a certain group of people that had access to the collected data.

European Court of Human Rights

1) *Klass and others v Germany* App no. 5029/71 (ECtHR, 6 September 1978)

Klass and others was one of the first cases in which the right to private life and data protection was balanced with counterterrorism actions.[281] The five applicants were lawyers, public prosecutors and judges[282] and they claimed that the Article 10 para. 2 of the German Basic Law and the statute on the Restrictions on the Secrecy of the Mail, Post and Telecommunications violated the Article 8 of the ECHR. These German laws have been legislated for monitoring of telephone calls and mail.[283] The claim stated by the applicants didn't concern the states right to have surveillance measures, but the lack of obligation to inform the persons concerned about the surveillance measures.

The ECtHR then stated that the German statute did interfere with the ECHR Article 8.[284] However, in its reasoning it stated that despite this interference, the German statute did not violate the ECHR Article 8.[285] The ECtHR stated that the German legislator was allowed to enact its above mentioned legislations in the way they have been enacted because of their necessity in national security and in prevention of crime.[286]

[281] *Boehm* 2012, p. 34.
[282] *Ibid.*
[283] *Ibid.*
[284] *Ibid.*
[285] *Ibid.*
[286] *Ibid.*

This case was an important milestone not only regarding the balancing of fundamental rights, but also regarding the legal processes.[287] The ground rule is that the applicant in court is the person who has been violated and in this case it wasn't.[288] This indicates that the so called victims aren't the only ones who can file up a case in court.

2) *Perry v the UK* App no. 63737/00 (ECtHR, 17 July 2003)

In this case, the applicant, Perry, was accused for multiple robberies and, because of this, was requested to attend an identification parade. The applicant refused this request. Because of this, the police placed cameras by the police station, which caught the applicants face. This camera footage was then shown to witnesses. Two of these witnesses identified the applicant as the thieve in these robberies. The applicant and his solicitor weren't informed about the usage of this camera footage and weren't given the opportunity to view the footage before it was used for identification matters.

Security cameras are obviously allowed in public areas, such as hospitals and shopping centres, where they serve public needs and security. However, in this case the camera was purposely adjusted so that it would only serve the purpose of the identification of a thieve and the case build against him. The recorded footage was also shown in court. The ECtHR judgement in this case concerned the question, whether these actions of processing and using of personal data interfered or breached with the fundamental right to respect for private life. As a conclusion, the ECtHR stated that these kind of actions interfered with the respect of private life and was not in accordance with the law and therefore there was a violation of Article 8 of the ECHR.

[287] *Boehm* 2012, p. 34.
[288] *Ibid.*

3) *S and Marper v UK* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008)

In these cases, both applicants had been suspects of a crime yet hadn't been convicted. Their fingerprints and DNA samples had been taken during the investigations. The fingerprints and DNA samples were stored in police records. Both of the applicants requested for the elimination of these data records, but the police refused. Because of this refusal, the case was taken into court and the ECtHR was requested for a preliminary ruling.

The ECtHR ruled that the storing of this kind of personal data was in fact violating the ECHR Article 8. The retention of fingerprints and DNA samples in this case breaches the ECHR Article 8, because there was no legitimate reason, such as crime prevention, for the retention of data. The applicants had been suspected for a crime, but hadn't been convicted, and weren't suspected for any other crime after that. For this reason, it was obvious that the police no longer needed the fingerprints and DNA samples of the applicants. The CJEU stated that "it was an entirely improper and prejudicial differentiation to retain materials of persons who should be presumed to be innocent".

4. Protection of personal data in international law

4.1. The United Nations (UN)

4.1.1. About the United Nations

The United Nations was founded in 1945 and it currently has 193 Member States.[289] It is an international organization that gives guidance and hosts negotiations in different kinds of situations, such as in fundamental and human rights issues.[290] This competence has been empowered by the Charter of the United Nations.[291]

The Charter of the UN (the Charter) came into force in 24th of October in 1945.[292] As stated above, the Charter states the principles and the responsibilities of the UN and is the foundational treaty of the UN.[293] It has Articles that concern, for instance, the economic and social co-operation, confirmation of peace and settlement of disputes.[294] It also regulates about the International Court of Justice and its status within the field of international law.[295] In addition to the International Court of Justice, the Charter regulates about other UN organs, such as General Assembly, Security Council, Economic and Social Council, Trusteeship Council and Secretariat.[296]

General Assembly is the main body of the UN and it is represented by all Member States of the UN.[297] General Assembly gather annually together to a session and a general debate, makes decisions concerning, for instance, new UN members and

[289] *United Nations*, http://www.un.org/en/sections/about-un/overview/index.html, read 26.3.2019.
[290] *Ibid.*
[291] *Ibid.*
[292] *United Nations,* http://www.un.org/en/sections/un-charter/introductory-note/index.html, read 26.32019.
[293] *Ibid.*
[294] *Ibid.*
[295] *Ibid.*
[296] *Ibid.*
[297] *United Nations,* https://www.un.org/en/sections/about-un/main-organs/index.html, read 26.3.2019.

elects every year a new General Assembly (GA) President to serve as a Speaker of the General Assembly.[298]

While the General Assembly, as can be assumed from its name, concentrates on multiple issues within the UN, other above-mentioned organs have more specific fields of work that they concentrate on. Security Council's responsibility is to maintain peace and security around the world.[299] Economic and Social Council is responsible for the international co-operation in environmental, social and economic issues and, also, the implementation of the acts that have been agreed in order to develop and maintain the international co-operation in these issues.[300] Trusteeship Council was at first established to work for the self-government and independence of certain territories.[301] These territories, however, had all reached independence and self-government by 1994.[302] After that, the Trusteeship Council changed its area of responsibility and, instead of concentrating on specific territories, it keeps an eye on the independence and self-government issues all over the world.[303] Finally, the Secretariat is the body which does the concrete work that have been pointed out by the other organs.[304]

These above-mentioned organs are those that have been regulated in the Charter of the UN. However, there are still multiple other bodies in the UN system, which are established for different tasks.[305] For now, I will only address those, which are relevant for this thesis. There are the Human Rights Committee, the Committee against Torture and the Committee on the Elimination of Racial Discrimination.[306] All these bodies have the right to take a stand on international violations of human rights that have been brought up by the victims of these violations.[307] For this thesis, the relevant body is the Human Rights Committee, which monitors the implementation of the International Covenant on Civil and Political Rights

[298] *United Nations,* https://www.un.org/en/sections/about-un/main-organs/index.html, read 26.3.2019.
[299] *Ibid.*
[300] *Ibid.*
[301] *Ibid.*
[302] *Ibid.*
[303] *Ibid.*
[304] *Ibid.*
[305] *Lewis-Anthony* 2016, p. 41.
[306] *Ibid.*
[307] *Ibid*.

(ICCPR).[308] Even though the individuals, a.k.a. the victims of the human rights violations, have the right to file a petition about these human rights violations to Human Rights Committee, the procedure is not as straightforward as it seems.[309] The ratification of the ICCPR does not itself guarantee the Committees right to take a stand on human rights violations that have been raised by the victims.[310] However,, the member states have informed that they acknowledge the Committees power to receive and consider the petition sent by a resident of a member states.[311]

Within UN, there is one more organ, which is relevant in this thesis, and it is the United Nations Human Rights Council. I shall tell more specifically about it, while introducing the Council's guidelines in Chapter 4.2.1.

4.1.2. The Universal Declaration of Human Rights (UDHR)

The Universal Declaration of Human Rights (UDHR) was the first international provision of human rights.[312] It was adopted by the General Assembly in 1948.[313] The UDHR was the starting point for the development of international, and also in some cases national, human rights laws.[314] Since it was the first international provision to declare that fundamental and human rights are applicable world widely and to all the people around the world, it has been, and still is, highly respected and referred international provision.[315] The UDHR is not legally binding, but, however, within customary international law it is recognised as having legally binding effect.[316]

[308] *Lewis-Anthony* 2016, p. 41.
[309] *Ibid.*
[310] *Ibid.*
[311] *Ibid.*
[312] *Colonna* 2016, p. 127.
[313] *Ibid.*
[314] *Ibid.*
[315] *Ibid.*
[316] *Ibid.*

The UDHR is quite general by its nature. It has 30 Articles which cover the basic human rights, such as the right to life, the right to liberty, the right to non-discrimination, the right to privacy etc. The Articles are quite short and pithy. For instance, compared to the CFREU and the ECHR, the Articles of the UDHR are much more uninformative than the Articles in the CFREU and in the ECHR even though they cover the same fundamental and human rights. Nevertheless, purpose of the UDHR is to, in a way, set the ground rules and be a provision that leads the way of human rights regulations. Unlike the CFREU and the ECHR and as I stated above, the UDHR is not legally binding. In my opinion, these facts explain its general nature and at the same time the way it has been written.

4.1.3. International Covenant on Civil and Political Rights (ICCPR)

International Covenant on Civil and Political Rights (ICCPR) came into force in 23rd of March in 1976. In its preamble, the individuals' rights to civil, political, social, cultural and economic freedoms have been emphasized, as well as the individuals' responsibilities towards other individuals and, also, states. ICCPR has altogether 53 Articles, which have been divided into six parts.

ICCPR includes many of the same rights that are also in UDHR, ECHR and CFREU, such as the right to liberty, the right to self-determination and the right to privacy. However, it does not have a specific right to property protection[317] nor does it have an Article for the right to data protection. Despite this, the UN Human Rights Committee, in its ICCPR General Comment No 16 in 1988, included data protection within the ICCPR. [318] ICCPR does not still have a specific Article for data protection, but it was included into the scope of the right to privacy.[319] As to the reason why data protection was included to the ICCPR, the UN Human Rights Committee stated that any sort of processing and collecting of personal data needs to be regulated by law.[320]

[317] *Lewis-Anthony* 2016, p. 43.
[318] *Kremer* 2017, p. 91.
[319] *Ibid.*
[320] *Ibid.*

4.2. Guidelines from international organizations

4.2.1. The United Nations Human Rights Council (HRC)

The United Nations Human Rights Council (HRC) is an inter-governmental body within the UN and was founded by the General Assembly on 15th of March in 2006.[321] Its task is to monitor human rights issues around the globe, take notice of these issues and then give guidance and set recommendations that base on the human rights issues and violations the HRC has came across with.[322] These recommendations, as can be suspected, are not legally binding.

The HRC gives an annual report, in which it has gathered decisions and resolutions about different human rights issues.[323] In its report A/70/53 from 2015, it has given a resolution concerning the right to privacy during digital age. In its introduction, the HRC brings up todays' challenges for the fundamental right to privacy, such as the technological developments and the increased usage of different technologies as well as the growth of internationalism. To support the fundamental right to privacy that has been regulated in the UDHR and ICCPR, the HRC decides in its A/70/53 report to appoint a special rapporteur. According to the report, the tasks of the special rapporteur are to gather and seek international and national information concerning the fundamental right to privacy. In addition, the special rapporteur ought to identify and give guidance to any difficulties within the protection of privacy. The special rapporteur should also raise awareness of privacy protection and, finally, give the HRC and the General Assembly a an annual report of all the relevant privacy related issues.

The report A/70/53 merely brings up the 21st century's challenges for the protection of privacy and creates a new system to follow the status of privacy protection and its development. The personal data protection is not discussed in this report. However, two years later in March 2017 the HRC brought up the right

[321] *OHCHR*, https://www.ohchr.org/EN/HRbodies/HRC/Pages/Home.aspx, read 26.3.2019.
[322] *Ibid.*
[323] *Ibid.*

to data protection in its resolution of report A/72/53. According to the report, the HRC advices all states to "review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law" and "to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data".

Both of these two reports had the same headline; "The right to privacy in digital age". It could be assumed from this, that the HRC sees the right to data protection as integral part of the right to privacy and not as an independent human right. Nevertheless, it clearly seems to me, that since the HRC especially brought the data protection up in its report, the HRC thinks it is an important issue and that international measures are in order for the individuals' right to data protection to be secured.

4.2.2. The Organization for Economic Co-operation and Development (OECD)

The Organization for Economic Co-Operation and Development (OECD) was founded in 1961 and it has 36 member states.[324] It works in co-operation with its member states to find effective solutions and guidelines for the development of economy and social issues in member states.[325] In addition, it takes measures to predict the future developments in different issues, such as environmental changes, economic developments and the effects of social changes to the people.[326]

[324] *OECD*, http://www.oecd.org/about/, read 27.3.2019.
[325] *Ibid.*
[326] *Ibid.*

The OECD has set guidelines on the Protection of Privacy and Transborder Flows of Personal Data and these guidelines were adopted in the 23rd of September in 1980.[327] These guidelines were revised in 2013, but they weren't fully altered and instead, a privacy expert group gave a report of the issues that should be revised, updated or considered.[328] In this report, the expert group has suggested updates and revisions mainly to the national privacy protection systems and, also, to the prevention of privacy violations.[329] In addition, the expert group highlights the importance of educating individuals about privacy issues and what individuals can do when facing privacy violations.[330] Because the 2013 review didn't make any profound changes to the guidelines, we shall concentrate on the original guidelines from 1980.

According to the preamble of the guidelines, many of the OECD member states have laws that protect privacy and also personal data as fundamental rights.[331] Member states have, for instance, regulated about the unlawful collection and processing of personal data and also about the unlawful disclosure of such data.[332] This is, of course, a positive development within the privacy and data protection. However, the differences between national privacy and data protection legislations may affect negatively on the transnational development in economic and social issues as well as on the free flow of data.[333] This realization is the reason why OECD member states thought that commonly accepted guidelines on privacy protection and transborder data flows were needed.[334] The goal of the guidelines is to harmonise national legislations in privacy and data protection of the OECD member states and, by this harmonization, to ensure the international economic and social development.[335] By achieving these goals, the international free flow of data can be secured.[336] For many member states, these guidelines have helped to

[327] *OECD* 1981, p. 1.
[328] *OECD* 2013, p. 1-12.
[329] *Ibid.*
[330] *Ibid.*
[331] *OECD* 1981, p. 5.
[332] *Ibid.*
[333] *Ibid.*
[334] *Ibid.*
[335] *Ibid.*
[336] *Ibid.*

modify their existing guidelines, but for other member states the guidelines have helped to create national privacy and data protection legislation.[337]

The OECD guidelines have five parts, which are the general part, the part of basic principles of national application and the parts of basic principles of international application: free flow and legitimate restrictions, national implementation and international co-operation.[338] The general part states the definitions for data controller, personal data and transborder flow of personal data.[339] The definitions are very similar to the definitions given in CFREU and ECHR. In addition, the general part tells the scope of application.[340] According to the guidelines, they apply to "personal data, whether in the public or private sector".[341]

In the second part are the basic principles of national application and the first is the principle of 'collection limitation'.[342] According to this principle, the collection of personal data should be limited by national legislation and, when personal is being collected, it should be done legally.[343] The second principle is the principle of data quality and according to it, the collected data should be up to date and relevant.[344] The third principle, the principle of purpose specification, is a bit similar to the data quality principle.[345] Only the data which is relevant for the purpose it has been collected for, can be collected.[346] Also the purpose for which the data will be collected, needs to be clarified before the data has been collected.[347] The principle of use limitation is the fourth principle and according to it, the purpose for which the data has been collected, cannot be widened without a legal authorization or the consent of the person whose data is in question.[348] Security safeguards principle requires reasonable protection for personal data against, for instance, unauthorized misuse or modifications.[349] The principle of

[337] *OECD* 1981, p. 5.
[338] *OECD* 1981, p. 9-12.
[339] *OECD* 1981, p. 9.
[340] *Ibid.*
[341] *Ibid.*
[342] *OECD* 1981, p. 10-11.
[343] *Ibid.*
[344] *Ibid.*
[345] *Ibid.*
[346] *Ibid.*
[347] *Ibid.*
[348] *Ibid.*
[349] *Ibid.*

openness requires that developments, practices and policies concerning data protection should be open and in line with the personal data protection regulations.[350] The last two principles are individual participation principle and accountability principle.[351] Individual participation principle grants the data subject the right to get information from the data controller.[352] The accountability principle sets out the data controllers responsibilities in controlling, processing and informing of the collected data.[353]

The OECD guidelines set the minimum principles for national data protection legislations of OECD member states, which are created to ensure the national and international data protection while also maintaining the economic, social and environmental development.[354] As only stating the minimum standards, the guidelines are not meant to be exhaustive and are instead meant to function in accordance with other international regulations and guidelines.

4.2.3. Others

In addition to the United Nations Human Rights Council and The Organization for Economic Co-operation and Development, there are globally many other international organizations. These are usually non-governmental organizations (NGO).[355] Many national human rights specialists, such as human rights lawyers, work together with international human rights NGOs, while helping individuals with human rights violations.[356]

These organizations vary greatly around the world.[357] They vary by their sizes, from one member to many million members, and by their area of focus; some concentrate on specific fundamental and human rights and others contrate on

[350] *OECD* 1981, p. 10-11.
[351] *Ibid.*
[352] *Ibid.*
[353] *Ibid.*
[354] *OECD* 1981, p. 28.
[355] *Hannum* 2016, p. 19.
[356] *Ibid.*
[357] *Ibid.*

specific residential area.[358] Many of the NGOs have decided to focus on specific human rights in order to gain expertise within these specific areas of human rights.[359] For instance, Amnesty International focuses on the human rights concerning human integrity.[360] Some other NGOs, such as the International Human Rights Law Group, have not limited their area of work within the human rights sphere.[361] These organizations work with human rights issues relating to any of the rights specified in international provisions.[362]

I searched for other NGOs and found, at least, the International Human Rights Council, the International Human Rights Committee and the International Human Rights Commission. According to their home websites, these all concentrate on specific human rights or territories. For that reason, the relevant guidelines in this thesis are those given by the HRC and OECD.

4.3. International human rights law

The international human rights law consists of multiple different legal sources, such as regulations, legislations and treaties.[363] There are also international organs that ensure the respect of fundamental and human rights all over the world.[364] The basic standard for international fundamental and human rights is that the nations world widely are required to respect the rights that have been granted to the people.[365]

The characteristic features concerning the international human rights law can be divided to at least four different parts.[366] The first is the fact that there are internationally over twenty legislations, regulations, treaties etc. concerning the

[358] *Hannum* 2016, p. 19.
[359] *Hannum* 2016, p. 20.
[360] *Ibid.*
[361] *Ibid.*
[362] *Ibid.*
[363] *Bilder* 2016, p. 3.
[364] *Ibid.*
[365] *Ibid.*
[366] *Bilder* 2016, p. 6-8.

fundamental and human rights.[367] These are only legally binding in those countries, which have singed and taken part of the statute.[368] One of these over twenty statutes is the United Nations' Universal Declaration on Human Rights (UDHR), which is the most important ground ruling for international fundamental and human rights and which has a binding, however not legally binding, status almost everywhere in the world.[369] Secondly, in addition to these above mentioned treaties and regulations, there are also many international guidelines and recommendations which aren't legally binding, but have an impact on the international fundamental and human rights affairs.[370] Thirdly, also the concrete actions taken by different international organs have protected the fundamental and human rights.[371] The fourth characteristic feature are the numerous national legislations and national jurisdictions.[372] These are extremely important for the implementation of international fundamental and human rights statutes to be in balance in nations and in uniform between different countries.[373]

Some of the challenges caused by the international regulations, treaties etc. have been already in this thesis, but one additional challenge is the fact that the international human rights law cannot usually be applied by an individual and is primarily applied by the states.[374] Generally, only states can file up a case in international courts.[375] Individuals can apply international human rights law and file a complaint only, if it has been accepted by the individuals state of residence.[376] For instance, 53 of the countries that are parties to the ICCPR have granted the individuals to file a complaint in international court if needed.[377] This amount of countries isn't a lot yet still better compared to different regions such as Africa and Asia, where the individuals haven't even been granted with the right to be heard in a legal case.[378]

---

[367] *Bilder* 2016, p. 6-8.
[368] *Ibid.*
[369] *Ibid.*
[370] *Ibid.*
[371] *Ibid.*
[372] *Ibid.*
[373] *Ibid.*
[374] *Bilder* 2016, p. 9.
[375] *Bilder* 2016, p. 11-12
[376] *Hannum* 2016, p. 29.
[377] *Ibid.*
[378] *Ibid.*

As I stated above, the international human rights law is legally binding only in those countries that are parties to different international treaties, statutes etc.[379] In addition of being binding sources of laws, these international human rights regulations work as sources for the national human rights regulations, which are often regulated in accordance with the international human rights regulations.[380] Some international fundamental and human rights treaties even require this kind of standardizing between national and international legislations.[381] One reason for this is obviously the willingness to unify the international and national human rights regulations, but also the fact that it is much easier to implement human and fundamental rights through national legislations.[382] For instance, it is much easier to file up a case in human rights violations in national courts than in international courts.[383]

The authority of international courts is generally dependent on the consents given by the relevant nations.[384] In addition, there is no international police who would enforce the international legal sphere and enforce the judgements given by the international court.[385] Like with the international human rights laws, the co-operation between international and national authorities is also required when these international human rights laws are implemented.[386] Only the human rights judgements given by the inter-American and the European courts have the authority to judge, for instance, damages on cases about human rights violations.[387]

While the world has developed, the international human rights law has developed as well.[388] However, it seems like the development in international human rights legislations doesn't quite keep up with the developments in economy, internationalism, technology and other developments in the world since the violations in fundamental and human rights, which originate from these

[379] *Bilder* 2016, p. 9.
[380] *Ibid.*
[381] *Bilder* 2016, p. 12.
[382] *Ibid.*
[383] *Ibid.*
[384] *Bilder* 2016, p. 11-12
[385] *Ibid.*
[386] *Ibid.*
[387] *Hannum* 2016, p. 29.
[388] *Bilder* 2016, p. 14-16.

developments, are still a daily struggle around the world.[389] The reason for this might be the differences in cultures and social features around the world, and it has been questioned, whether nations all over the world with different kind of cultural and political backgrounds truly can find an uniform international human rights legislation and commit to that?[390]

This is not a simple question as can be seen from the different aspects of international human rights law stated in this thesis. It might be so that the answer to the previous question is no. However, it is also relevant to question whether it is required to have this kind of uniform international human rights law. Maybe the relationship and co-operation between the international and national level and also the co-operation between the two major human rights sources, the EU law and the international law, are sufficient enough. Of course, the relationship between the EU law and international law hasn't always been that friendly as can be seen from the following chapter.

4.4. EU law vs. international law

The technological developments that started in the 1970s were the kickoff for the data protection regulations in Europe and within the EU and of course all around the world as well.[391] However, the data protection legislations and other regulations enacted in the 1980s and in the 1990s aren't sufficient enough in this modern world, which is why the data protection regulations in the EU and around the world are being revised.[392] These revisions ought to be done in accordance with the technological developments, but also keeping in mind other relevant connections, such as national security and surveillance to which data protection is closely connected to.[393]

[389] *Bilder* 2016, p. 14-16.
[390] *Ibid.*
[391] *Kiss – Szke* 2015, p. 227.
[392] *Ibid.*
[393] *Kremer* 2017, p. 85.

The EU has a good range of fundamental and human rights regulations and also data protection regulations.[394] These are internationally the most strict regulations and have a legally binding status.[395] When an organization, for instance, falls under the scope the EU legislation, this organization is required to comply with multiple different requirements, which have been enacted in the EU legislation.[396] For instance, many countries outside of the EU, such as Canada and Argentina, amended their national privacy and data protection legislation in order it to be coherent with the EU data protection directive.[397] Also Norway and other European Economic Area countries were required to adapt with the EU data protection directive.[398] However, the EU data protection laws haven't spread to all countries all over the world. For instance, China doesn't have any laws concerning data protection nor privacy and Russia hasn't yet ratified its data protection and privacy laws, which aren't even coherent with the EU laws.[399] The strictness of the EU data protection laws and regulations can be seen, for instance, from the restrictions it has set for the countries that don't have adequate data protection regulations.[400]

The international law, on the other hand, doesn't have the same impact and isn't legally binding, and basically only sets out international guidelines and recommendations. As stated above, international human rights law is dependant on the nations and their national legislations all around the world. One example of these guidelines are the requirements for a new fundamental and human right that have been set in the international level.[401] These minimum requirements for a new fundamental and human right are that it

- is required to have social value;
- must be relevant;
- must be as in accordance with existing fundamental and human rights as possible;

[394] *Ustaran* 2013, p. 137.
[395] *Ibid.*
[396] *Ibid.*
[397] *Heisenberg* 2005, p. 103.
[398] *Heisenberg* 2005, p. 106.
[399] *Ibid.*
[400] *Bygrave* 2002, p. 79.
[401] *Tzanou* 2017, p. 18-19.

- must be formed precisely.[402]

Data protection issues have had significant impact on the relationship between the EU law and the international law.[403] The reason for this is that the personal data has an important role in the development of international economy and technology, and which is also why the data protection laws have evolved during the last years in the EU and in the international level as well.[404] For instance, already in 1990 when the computer age really took off, the UN gave recommendations for regulations concerning viral personal data.[405]

Data protection issues have raised questions, discussion and even conflicts during the recent years. In 2003, a data protection related conflict arose between the EU and the United States.[406] In that year the US ratified a law for the prevention of terrorism.[407] According to this law, the Department of Homeland Security in the US was allowed to have the personal data, which had been gathered for commercial use, about the passengers coming to the US.[408] Because the purpose of use was changed from commercial reasons to national security, it had to comply with the EU data protection directive when EU residents travelled to the US.[409] This US law and demand on getting such data violated the EU data protection directive.[410] The EU negotiated with the US and in 2004 they ended up on writing an agreement, which would grant the US a permission to collect this data for the means of national security, but which would also obligate the US to provide a sufficient protection for the collected personal data.[411]

The relationship and co-operation between the EU and the US have significant impact to the rest of the world. There are nearly 800 million people living in the EU and the US that are directly affected by the decisions made by these two major

[402] *Tzanou* 2017, p. 18-19.
[403] *Kremer* 2017, p. 91-92.
[404] *Ibid.*
[405] *Terwangne* 2009, p. 183.
[406] *Heisenberg* 2005, p. 1.
[407] *Ibid.*
[408] *Ibid.*
[409] *Ibid.*
[410] *De Hert – Gutwirth* 2009, p. 33-34.
[411] *Ibid.*

operators.[412] Despite this above mentioned conflict in 2003-2004, the EU and the US have co-operated remarkably with personal data transfers when they are connected to criminal issues.[413] This co-operation has been strengthen with multiple different agreements between the EU and the US, such as the Interim Agreement, which ensures the finance tracking of terrorists in the EU and the US.[414]

Despite this co-operation, it is almost impossible to specify the legal authorities within the legal co-operation between the EU and the US.[415] This fact brings its own risks, when the different interpretations of the above-mentioned agreements might cause conflicts.[416] To avoid these kind of conflicts, a clarification for the interpretation of these agreements or a pointing of a supervisory authority, which would control the interpretation of the agreements, could be in order.[417]

Stefano Rodotà has wrote in his article *Data Protection as a Fundamental Right,* from 2009, that the modern world requires a genuinely international constitution with fundamental and human rights regulations.[418] Rodotà thinks that especially the fundamental rights of freedom of expression and the personal data protection are needed all around the world and require international, constitutional level, regulation.[419] I actually agree with Rodotà with some restrictions, which I will tell more about in the second and, at the same time, the final chapter.

[412] *De Busser* 2012, p. 185.
[413] *Ibid.*
[414] *Ibid.*
[415] *De Busser* 2012, p. 188-189.
[416] *Ibid.*
[417] *Ibid.*
[418] *Rodotà* 2009, p. 82.
[419] *Ibid.*

5. Conclusions

As I recall from the history lessons in high school, the history of human rights goes all the way back to the time of revolution and especially to the French revolution in the 18th century. Back then, the main goal was to get rid of the class differentiation and to grant the general fundamental and human rights, such as the right to live, to all people. Now, in the 20th and the 21st centuries, these general fundamental and human rights are enjoyed all over the world, at least should be, and new fundamental and human rights have been developed. The right to personal data protection is one of these new rights.

What is then personal data? In the US, the personal data has been divided into personally identifiable and non-personally identifiable data.[420] The personally identifiable data are the name, email address, home address, birthday and social security number of the data subject, while the other information falls under the scope of non-personally identifiable data.[421] However, this division is under revision.[422] In Europe and in the EU the viewpoint to personal data is a lot more strict, as have been noted before. In the EU, the personal data has been defined as any data that can be connected to the data subject and by which the data subject can be identified.[423] With such a broad definition it can be ensured that the new ways of processing personal data fall under the scope of personal data protection laws.[424]

Fundamental and human rights are made for the people and meant for the people. That is why they should be as clear as possible without any complex legal wordings or terms.[425] Sometimes, however, the wording of a fundamental right and the way it should be interpreted isn't that clear. The right to private life, in other words the right to privacy, and the personal data protection are good examples of this. The area of interpretation, content and the precedence compared to other fundamental rights aren't always clear. As can be seen from the cases presented in chapter 3.3.

[420] *Chester* 2012, p. 56.
[421] *Ibid.*
[422] *Ibid.*
[423] *Colonna* 2016, p. 28.
[424] *Colonna* 2016, p. 29.
[425] *Markou* 2015, p. 164.

and from the other parts too in this thesis, the personal data protection is often seen as part of the right to privacy. This happened, for instance, in the case of Promusicae, in which the CFREU was interpreted and which has its own Article for personal data protection.

In addition to this, the fundamental right to personal data protection is very often seen as a secondary right compared to other fundamental rights.[426] Because personal data protection is under continuous threads, this order of precedence should be adjusted more carefully.[427] Breaches and violations on someone's personal data can cause serious harm to the data subject. This harm can be much more serious and, also, expensive for the data subject than a violation on someone's right to the freedom of speech. At least on my opinion.

As I said before, compared to other fundamental rights, the right to personal data protection is seen as a new right.[428] Despite its newness, it is extremely relevant in this modern world with its developments in technology, economy and other.[429] One of these developments is the possibility to use personal data as a currency.[430] Personal data can also work as a tool for decision-making or as a code and because of these developments, it is even more important to decide on the status of the personal data protection; is it a fundamental right or not?[431]

I think the personal data protection is in a way a fundamental right. It has been regulated in the CFREU as a fundamental right and some of the legal scholars sees it as a fundamental right. In the EU legal system, the personal data protection has been recognized, at least in theory, as a fundamental right.[432] The reason for this lies behind the challenges and threads personal data protection faces, which I have gone through in this thesis.[433] However, in legal praxis and in other international and national regulations, legislations and treaties its status as a fundamental right isn't as clear.

---

[426] *Rodotà* 2009, p. 80.
[427] *Ibid.*
[428] *Kremer* 2017, p. 102.
[429] *Ibid.*
[430] *Ibid.*
[431] *Kremer* 2017, p. 103.
[432] *De Hert – Gutwirth* 2009, p. 8.
[433] *Ibid.*

Even according to the Finnish constitution, the status of personal data protection is unclear. According to the right to privacy in Finnish constitution, its purpose is to protect the private life, honour and security of home. In this same paragraph it has been stated that the personal data protection has been regulated in secondary legislation. This gives room for various interpretations.[434] Why has it been stated within the paragraph of fundamental right to privacy if it has been legislated in secondary legislation? Should it be interpreted so that it is a fundamental right as part of the right to privacy and the secondary legislation about the personal data protection supports the fundamental right? Or should it be interpreted so that it isn't part of the fundamental right to privacy and should be considered as a regular right and which has been regulated in secondary legislation?

The Finnish constitutional doctrine might give an answer to this. According to this doctrine, data protection is part of the fundamental right to privacy.[435] In addition, the Finnish Constitutional Committee has given a statement (PeVL 21/2012 vp) where it highlights the importance of protecting data protection in a way, which is in accordance with the fundamental rights system.[436]

The relationship between the protection of personal data and the right to privacy and private life is still under debate while at the same time these fundamental rights have even been seen as synonyms.[437] The differentiation between these two rights has even been seen as a rather theoretical ideology that does not adapt to the legal praxis.[438] However, the ideology about synonymity can be too restrictive and some scholars have presented the ideology of the parity of privacy and data protection.[439] In Finland, legislation and legal praxis lean on the ideology of parity[440], which differs from the European version, where, for instance in France and Germany, the data protection is its own fundamental right and is rationalized with intellectual self-determination and not with the right to privacy.[441]

---

[434] *Koillinen – Kulla* 2014, p. 116.
[435] *Ibid.*
[436] *Koillinen – Kulla* 2014, p. 118.
[437] *Koillinen – Kulla* 2014, p. 115.
[438] *Ibid.*
[439] *Ibid.*
[440] *Ibid.*
[441] *Koillinen – Kulla* 2014, p. 116.

Despite all these different theories and ideologies about the status of the protection of personal data, it has clearly been agreed almost all over the world that there really is a need for international personal data protection regulation. With the afore mentioned developments and challenges, and with the collecting and storing of peoples' personal data, political decision for more detailed and more specific data protection regulations are required.[442] Even though new laws and regulations are in order, it might be, however, that the required changes are only made to the existing legislations and regulations.[443]

While making these political decisions, the international data protection principles should be taken into account.[444] The data protection principles, which are alike with the principles of restricting fundamental and human rights, are that the personal data should be collected and processed lawfully and for a specific reason.[445] In addition, the collected data must be deleted when it is no longer needed and the data subject must give his or her consent before his or her personal data can be collected or processed.[446]

The findings of legal scholars support the need for consistent international data protection legislation.[447] Legal scholars have stated that "every data processing duplicates the risk of abuse of the relevant information".[448] Automatic processing of data is advanced yet still risky; the data may end up in a wrong database, some important and relevant information might be deleted, and when the data is no longer needed it won't be deleted at all.[449] All of these issues may cause serious harm to the data subject.[450]

The differences between different kind situations concerning personal data protection is a challenge for enacting data protection laws.[451] It might be impossible to enact an international data protection law that could be interpreted

[442] *Selmer* 1990, p. 18.
[443] *Heisenberg* 2005, p. 103.
[444] *Tzanou* 2017, p. 13.
[445] *Ibid.*
[446] *Ibid.*
[447] *Boehm* 2012, p. 20.
[448] *Ibid.*
[449] *Ibid.*
[450] *Ibid.*
[451] *Pagallo* 2012, p. 342-344.

in every issue concerning personal data protection and which would give a solution to any problem related to data protection.[452] What would be then the best way to legislate personal data protection?

Throughout this thesis I have mainly represented the facts, laws and legal theories I have found from different sources, such as legal literature and sources of law. Now I shall address my own ideologies and theories about the personal data protection.

As I mentioned before, I see the personal data protection as a fundamental right. I base this opinion to the legislative developments, legal theories and legal praxis concerning personal data protection, and, in addition, to my own observations. However, its status as a international fundamental right hasn't yet been officially confirmed. There are of course the data protection Article in the CFREU and, also, the recommendations from international organizations, but these aren't enough to give the data protection an international status as a fundamental right.

Another question is, however, whether the personal data protection needs to be a fundamental right or whether it is enough that the personal data protection is regulated in secondary legislation. I think that personal data requires the protection, which the fundamental rights regime, principles and theory guarantees. As has been made clear in this thesis, the personal data faces threads and challenges everyday internationally and nationally. The developments in technology, internationalism and economy, and the inconsistency in international data protection legislation all causes these threads and challenges. Because the personal data is a sensitive information and violations and breaches of someone's personal data can cause serious harm, and, also, because the threads and violations occur daily, I think that personal data of a data subject should be protected with the principles and status of a fundamental right.

However, as I brought up before, the personal data protection hasn't officially got its status as an international fundamental right. What should then be done? The Universal Declaration of Human Rights (UDHR) should be revised and the new

[452] *Pagallo* 2012, p. 342-344.

fundamental and human rights, such as the personal data protection, should be added into it. If personal data protection would be added into the UDHR, it would have an international impact on its status as a fundamental right just because the UDHR is the most significant international human rights declaration. Even though in the EU the data protection regulations have been revised during the recent years, also the ECHR requires revision. When the other fundamental Charter in the EU, the CFREU, is legally binding and has a separate Article for personal data protection, should also the ECHR have a separate Article for personal data protection. I think this way, because the ECHR and the CFREU are applied to similar cases and within the same jurisdictional area. The more unified the legislations are in a specific jurisdictional area, the clearer the legal praxis and the applied regulations and legislations are.

The revision and standardizing of international legislations, charters, regulations, agreements etc. isn't that easy. If it was easy, it probably would have been done already. Cultural differences, national legislations and other national characteristics makes this process of revision and standardizing harder. However, I still believe that it is still possible to create some kind of international fundamental right to data protection, which grants the personal data the required protection, but isn't too strict and honors the cultural differences around the world.

The question about the destiny of personal data protection and about its international legal status might not get a definite answer in many years. It seems to me that international legislations etc. aren't revised frequently even if the revision would be needed. It also seems like the international legal systems and sources of laws are always one or two steps behind the changes and developments surrounding it. For now, it remains unseen, how does the international legal instruments answer to the personal data protection issues.