TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Kristina Rutšjevskaja

TELECOMMUNICATIONS DATA RETENTION REGULATIONS AND CRIMINAL INVESTIGATIONS - SOLUTIONS FROM THE FINANCIAL SECTOR

Bachelor's thesis
Programme Law, specialisation European Union and International Law

Supervisor: Dr Agnes Kasper, PhD

Tallinn 2020

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 9301 words from the introduction to the end of conclusion.

Kristina Rutšjevskaja ……
(signature, date)
Student code: 164920HAJB
Student e-mail address: kristinarutsjevskaja@gmail.com

Supervisor: Dr Agnes Kasper, PhD:
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

The always evolving technology is a headache for lawmakers, who are in a constant race to catch up with and regulate the latest industries and advancements within them. The European Union is finally managing to catch up with the rapidly developing industries by imposing proper regulations in order to protect consumers, while also enabling law enforcement to use the vast amounts of data collected by these service providers for conducting successful criminal investigations. One such industry, the Telecommunications (Telecom) sector, is particularly problematic, whereby the amount and nature of data the service provider can gather, access and keep for years is regulated poorly in a way that is in conflict with privacy of its customers and does not sufficiently serve the law enforcement. The Telecom sector can potentially provide crucial information to aid criminal investigations by providing retained data about a suspect. However, because data retention in the sector is currently poorly regulated, it neglects much needed safeguards and lacks a harmonized European framework in order to be both effective in aid crime fighting and proportional in a democratic society. In contrast, the Financial sector has very clear regulations that help law enforcement to successfully conduct criminal investigations while respecting customers data. This thesis examines the legal challenges the Telecom sector is facing in regards data retention for criminal investigations and aims to provide solutions based on the Financial sector effective crime-fighting legal framework.

Keywords: Privacy, Telecommunications, Data Retention, Financial Sector, Criminal Investigation, European Union.

INTRODUCTION

Communication confidentiality is a fundamental right[1]. In the middle ages it was regarded as a privilege to be able to receive postage, and once countries in Europe realised the potential of economic value in postage business, they began to nationalise it. The Telecom sector also got nationalised later on and similarly to the postage system, was seen as an exclusively governmental business.[2] The nineteenth century was an important time where a lot of rights got constitutionalised, among them the right to remain confidential in correspondence. In addition, after World War II, the right to confidentiality in correspondence was allocated under the right to privacy in the European Convention on Human Rights (ECHR)[3] and included in its provision the right to privacy in new communications types such as communication by telephone.[4]

With the emergence of the Internet and new technologies it has become apparent that privacy as a right is harder to balance with requests for data for various purposes. Nowadays, a lot of people use a smartphone, computer or have access to the Internet, which means that each time they call, message or use any other services on phone or the Internet, a significant amount of data is created and retained by various service providers. Such data includes call and location logs, message history and content like photos and videos, created by service users. When such data exists and is readily available, it can be used for solving crimes by allowing the law enforcement or relevant parties to access retained customer data to use as evidence. To achieve that, there must be a balance between respecting a person's privacy while accessing the person's retained data for criminal investigations. In a world where the majority of the population is on the Internet, data is a valuable asset to retain and use, especially if it provides means to solving crime.

---

[1] European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), article 8. Accessible: https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=

[2] Borgesius, F.J.Z., Steenbruggen, W. (2018). The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust. *Theoretical Inquiries in Law, Forthcoming*, 19 (2), 293.

[3] European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), *supra nota* 1, article 8.

[4] Borgesius, F.J.Z., Steenbruggen, W., *supra nota* 2, 296.

However, privacy is not an absolute right according to the ECHR, meaning, the Telecom sector may collect and store data if it is in accordance with exceptions listed in Article 8 of the Convention[5]. Therefore, if the law is proportionate and the information helps to prevent crime or contribute to public safety, there should be no issues regarding retaining and sharing the data for such purposes. The problem lies with the Telecom sector's struggle to balance proportionality with the right to privacy, thus failing to create effective legal frameworks of data retention for criminal investigations.

The author takes a heavily regulated Financial sector to compare with the Telecom sector. The Financial sector has been one of the sectors alongside the Telecom sector that were used to collect large amounts of data since the 1970s forward.[6] The Financial sector is facing similar issues with new emerging technologies[7] and it has data retention within AML/CTF[8] framework that has been adopted by the European Union[9]. In contrast, it clearly outlines when the financial institutions need to provide specific information in order to prevent crime or assist in criminal investigations, such as which data points are collected from customers, by whom, and how long the data should be retained in specific cases.

The main question of this thesis is, how, if at all, can financial sector's data retention principles help to close the legal gaps found in Telecom sectors policies? The author's aim is to find potential solutions based on the comparison between the Telecom and the Financial sector and make suitable recommendations for building a harmonised European data retention legislation in the Telecom sector.

Telecom sector's legal gaps are identified by examining the relevant policies and cases on data retention. The identified legal gaps lead to the hypothesis that the Telecom sector's data retention laws should be reformed. The Financial sector's data retention regulations are designed to be concise, proportionate and practical when aiding in criminal investigations, therefore they could serve as a model for designing a data retention regime in the Telecom sector. Creating a legal framework for the Telecom sector on the basis on Financial sector's data retention principles could

---

[5] European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), *supra nota* 1, article 8.

[6] Bignami, F. (2007) Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law*, 8 (1), 234.

[7] OJ L 337, 23.12.2015.

[8] Anti-Money Laundering and Counter-Terrorism Financing

[9] OJ L 141, 5.6.2015.

provide a more effective and fair system for preventing, conducting and prosecuting criminal matters.

The author chose this topic of immediate relevance to examine the regulatory framework and cases surrounding Telecom services and identify the legal gaps, in order to determine solutions for the sector for a new approach in data retention rules. Doctrinal legal research is used as a method to interpret relevant regulations in both sectors, as well as having the relevant case-law analysis in order to understand the topic. Comparative legal research is used to compare data retention regulations from two above mentioned sectors and find differences between them.

The author first examines the past and current data retention laws in the European Union. The aim of this analysis is to understand the topic of data retention in the Telecom sector. The author then examines the legal challenges concerning privacy, data retention and proportionality when conducting criminal investigations. Then, an examination of how data is retained in the Financial sector for criminal investigations will provide insight that will allow the author to compare two sectors. By understanding the data retention issues in the Telecom sector and analysing the Financial sector's success the author can draw parallels and recommend a set of proposals for what principles the policymakers aiming to regulate Telecom sector could apply.

The Thesis is divided into 6 parts. The first chapter defines data retention, the main subject of this thesis, and provides background information about the Telecom sector and its difficulties in defining the modern communication services.

The second chapter provides a broader context needed for analysing legal gaps in data retention legislation. Data Retention Directive and the cases against it will be examined in this chapter, providing a background for data retention issues, as well as rules of the E-Privacy directive, and European Electronic Communications Code.

The third chapter analyses legal challenges of data retention for criminal investigations in the European Union Telecom sector, where the author analyses the data retention principles that need to be considered to retain the data proportionally in a democratic society.
The fourth chapter looks at data retention laws in the Financial sector and how the justified rules for criminal investigation purposes have been designed. The Financial sector's laws are observed in more detail and the criteria for a successful data retention framework are identified.

The fifth chapter compares data retention in the context of criminal investigations in both sectors in order to draw parallels, analyse and form conclusions from previous chapters findings. In this chapter the author proposes recommendations for the Telecom sector from the outcome of the analysis and the comparison with the Financial sectors data retention principles, criminal investigation procedures, and concludes the topic of this thesis.

1. TELECOMMUNICATIONS SECTOR AND DATA RETENTION

The Telecom sector consists of a variety of different types of communications services. The International Telecom Union defines Telecom as ‘’Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.’’[10]

The Telecom sector used to be a regulated monopoly of a few service providers offering services such as telephone or satellite among others, providing what was essentially message carriage over physical distance.[11] However, with the rise of Internet and more advanced systems the world has seen a major technological leap - there are now several new systems of message transmission available, such as wireless networks, packet communications and the Internet itself, which have significantly lowered the cost of communications in addition to throwing the traditional Telecom sector from a monopoly into a diverse and competitive market.[12]

European legislation established its own terminology, and rather referred to ‘electronic communication networks and services’ in Directive 2002/21/EC (Framework Directive),[13] further expanding and refining the scope of the regulatory framework in Directive (EU) 2018/1972 (European Electronic Communications Code).[14]

[10]Constitution of the International Telecommunication Union, Annex, p. 65. Accessible: https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx
[11] Black, S. (2001). Telecommunications Law in the Internet Age. *San Francisco: Elsevier Science & Technology*, 1.
[12] *Ibid*, 2.
[13] OJ L 108, 24.4.2002
[14] OJ L 321, 17.12.2018

1.1. Modern unclassified services under Telecommunications regulations

According to Article 2 (c) of the Framework Directive, which defined electronic communications service, the core factor determining whether a service falls within the scope of the framework was the conveyance of signals. Although the competition has made the market more innovative and cheaper, the emergence of new technologies has caused a discord between the old and the new service providers. Until now, the new communication service providers such as Facebook Messenger, WhatsApp, Instagram chat and Skype were able to use methods of communication in their product and not be bound by the same compliance rules as traditional electronic communications service providers, since arguably these providers are not in the business of signal conveyance. However, Article 2 (5) of the European Electronic Communications Code considerably extended the meaning of electronic communications services, thereby bringing into the framework's scope interpersonal communication services as well, which is a significant addition to the services that in essence consist of signal conveyance. The key issues that cause this delay in regulation are global nature of communication, not adhering to clear jurisdiction (service provider customers are often in another country), and lack of modern definition of what constitutes as Telecom service in the age of borderless and fast-paced Internet environment.[15] The fact that these new electronic communication services have now been classified under the same umbrella shows that the policy makers finally have a good time to start creating better legislation that can apply to the old and the new services alike, harmonizing the way data is handled.

1.2. Data retention within the Telecommunications sector

Privacy and data protection are arguably two of the most important human rights[16] of today's world.[17] It is then problematic to see how communication technologies are actively undermining these two important human rights by providing the means to collect, process and ultimately store the data. The more such storing and processing of individual data is done the more it can be accessed and managed by not only government agencies but also by businesses.[18] Thus, this

[15] *Ibid*, 389.
[16] European Convention for the Protection of Human Rights and Fundamental Freedoms, (1950), *supra nota* 1, articles 7 and 8.
[17] Friedewald, M., Pohoryles, J. (2013). Technology and privacy. Innovation. *The European Journal of Social Science Research*, 26, 1.
[18] *Ibid.*

creates a trust issue between the customers and the data processors, who use customer data for various purposes without proper safeguards. This means that the legislative innovation needs to walk alongside with these emerging technologies in order to be able to govern these innovations well.[19]

One of the issues standing in the way of people exercising their right to privacy and data protection is the data retention rules in specific sectors, such as the Telecom sector. It is important to make a distinction between data retention and data preservation, though, as they are not the same. According to the Convention on Cybercrime,[20] data preservation happens not as a regular requirement to retain the data continuously, but to extract specific existing data on a case-by-case basis upon request from law enforcement. This means that no data is kept or retained, but any data only in the present moment can be requested for examination. Therefore, data retention is an obligation to retain information within a specific timeframe, regardless whether there is a request for it or not. It can be concluded that data retention is a collection of specified data points about users retained for a certain period of time in order to be accessible to the law enforcement.

The history of more conservative data retention practices in the Telecom sector is not that distant, the first data retention legislation on the European Union level being introduced in 1997 in the form of Directive 97/66/EC. It was used as a non-mandatory instrument to aid the Telecom sector with criminal investigations process, however it was shortly replaced by e-Privacy Directive in 2002, which laid down more specific provisions and set out mandatory obligations for service providers in the sector.[21] Shortly after, the United Kingdom convinced the EU to pass a more strict Directive regulating data retention for criminal investigation purposes after the 2005 London and Madrid terrorist attacks.[22]

Since then, Telecom services have been providing law enforcement with significant amounts of customer data by lawful means,[23] but it has not been without struggles to harmonize the sector's laws: from invalidating a whole legal instrument to implementing new laws on both national and

[19] *Ibid.*

[20] ETS. 185 Budapest Convention on Cybercrime.

[21] Dusanovic, D. (2010). Implications of Invalidity of Data Retention Directive to Telecom Operators. *Juridical Tribune*, 4 (2), 45.

[22] Brown, I. (2010). Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology*, 19 (2), 96.

[23] *Ibid*, 100.

European Union level in recent years, such as the General Data Protection Regulation and the European Electronic Communications Code.

The following sections will provide insight into the problems that the Telecom sector is currently facing and what can be learned from the legal instruments of the past and present.

2. DATA RETENTION LEGISLATION DEVELOPMENTS IN TELECOMMUNICATIONS SECTOR

The following chapter analyses different legal instruments concerning data retention and see what legal gaps can be found within them in the Telecom sector, in order to compile a set of principles that need to be satisfied in order to create proportionate and transparent legal framework pillars for a data retention legislation proposal.

This is done by analysing the Data Retention Directive[24] and cases against it that eventually helped to declare the problematic Directive null and void, as well as exploring current e-Privacy Directive and the European Electronic Communications Code and their impact on data retention for criminal investigations.

2.1. Data retention directive 2006/24 and its invalidation

The Telecom sector had already been retaining customer data for a short amount of time for billing purposes, however it was in the early 2000s when the European Union realized that this data could be valuable for criminal investigations and thus introduced some form of provisions into national legislation.[25]

Since the London bombings[26] of 2005 the Member States were on the consensus that there needed to be a common, unified legal framework allowing law enforcement to access certain data points in order to ensure public safety. The political climate at the time seemed to have shaped the now invalidated Directive into a drastic measure to fight crime and departed greatly from data protection that was mandated by then-effective Data Protection Directive and e-Privacy

[24] OJ L 105, 13.4.2006.

[25] Eisendle, D. (2014). Data Retention: Directive Invalid - Limits Imposed by the Principle of Proportionality Exceeded. *Vienna Journal on International Constitutional Law / ICL Journal*, 8 (4), 458.

[26] OJ L 105, 13.4.2006, preamble (10).

Directive.[27] Since then, the Data Protection Directive has been updated by 2016 General Data Protection Regulation (GDPR).[28] Additionally, the Police Directive 2016/680[29] was adopted alongside GDPR as a means to regulate the access of retained data of individuals by the law enforcement, making the authorities accessing the retained data be bound by the law. In this regard the GDPR has an effective measure of regulating the authorities conduct and binding them to abide by law within each Member State.

Certain provisions in the newly adopted Data Retention Directive made people more aware of their usage of devices governed by the Telecom sector and brought about a threat to their privacy. In the next section the author will analyse the two of the most influential cases that helped invalidate the problematic Directive in 2014 and define what conditions were advised by the Court to be met for any future legislation on this matter to be successful.

2.1.1. Cases against data retention directive – Digital Rights Ireland

One of the most important cases against the Data Retention Directive were the joined cases C-293/12 and C-594/12, collectively called Digital Rights Ireland. The case called for interpretation of Articles 3, 4 and 6 of the Directive, whereby the articles were in violation of the European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950. Articles 7, 8, 11 and 41[30] and defined clearly why the Directive was not allowed to be in effect and what principles did future data retention policy makers need to follow.

The Court found several shortcomings of the Directive: 1) it violated the fundamental human rights of all European Union citizens by imposing a blanket data retention without them being notified of access to their data by other persons[31] thus 2) putting them under fear of being under constant surveillance[32], 3) key elements of data retention and usage were left to the Member States to define, for example ‘’serious crime’’ was not defined so it was unclear when law enforcement can access

[27] Feiler, L. (2010). The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. *European Journal of Law and Technology*, 1 (3), 2.
[28] Black (2001), *supra nota* 11, 61.
[29] OJ L 119, 4.5.2016, p. 89–131
[30] Judgment 8.4.2014, C-293/12 and C-594/12, ECLI:EU:C:2014:238
[31] Munir, A.B., Yasin, S.H.M., Bakar, S.S.A. (2017). Data Retention Rules: A Dead End. *European Data Protection Law Review*, 3 (1), 75.
[32] Eisendle (2014) *supra nota* 25, 459.

the data and on what conditions[33]; thus 4) being in breach of the principle of proportionality; 5) service providers only need to adhere to a ‘’minimum’’ level of security standards, which increases the risk of the retained data to be accessed without authorization or misused[34], thus there needs to be safeguards in place against improper or arbitrary use and interference of public authorities in terms of person’s data[35] ; 6) the Directive did not explicitly define the term ‘data retention’ but rather defined data vaguely as ‘’traffic data and location data and the related data necessary to identify the subscriber or user’’[36], instead leaving the Member States to define it themselves; 7) the data retention period was too vague, ranging anywhere between six months to two years[37] ; 8) the Directive does not provide any exceptions to the persons or type of communication that should be excluded from data retention, for example subjects to professional secrecy[38]; 9) there is no codification of procedure for accessing the data[39] and 10) it is not defined who are the ‘’competent authorities’’ who can access the data[40].

The judgment of the Court shows that for the regulatory framework to be effective it needs to not only be proportionate but also clearly defined in the principles that govern data retention - different elements such as who can access data, on what occasions and what type of data can be accessed. Safeguards such as accountability of the persons that can access and use the data need to be defined. The author argues that the points brought out by the Court about the inconsistencies within the Directive can be used as a foundation for the new potential legislation for data retention in the Telecom sector.

2.1.2. Cases against Data Retention Directive – Tele2

The joined cases C-203/15 and C-698/15 collectively called Tele2[41] were the second important case law that contributed to invalidating the Directive, as well as provided more concise

---

[33]Judgment 8.4.2014, C-293/12 and C-594/12, ECLI:EU:C:2014:238, *supra nota* 29.
[34]Vedaschi, A., Lubello, V. (2015). Data Retention and Its Implications for the Fundamental Right to Privacy. *Tilburg Law Review (Gaunt)*, 20 (1), 21.
[35]Breyer, P. (2005) Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. *European Law Journal*, 11(3), 367.
[36]OJ L 105, 13.4.2006, article 2 (1).
[37] *Ibid*, Article 6.
[38]Munir, Yasin, Bakar (2017), *supra nota* 31, 75.
[39]Vedaschi, Lubello (2015) *supra nota* 34, 22.
[40] *Ibid*, .27.
[41]Judgment, 21.12.2016, C-203/15 & C-698/15, EU:C:2016:970.

interpretation of the E-Privacy Directive[42] which took the place of the newly declared void Data Retention Directive.

While Digital Rights Ireland had set out concerns for a legal instrument of the European Union, the Tele2 cases concerned the national legislation level. The issue brought up was that after the Ireland case CJEU had decided there should be no blanket data retention law, however many of the European Union Member States had already implemented the Data Retention Directive in smaller or larger amounts. The Swedish Telecom provider Tele2 Sverige AB refused to retain data, arguing the flawed Directive's data retention laws imposed on the national level should not be applicable.

The judgment of the case concluded that general collection and retention of all subjects data is in conflict with the fundamental rights articles 7, 8, 11 and 52(1). Thus, the Court required the data retention not be general, but targeted and based on evidence of risk of crime being committed,[43] thus protecting the innocent persons from constant surveillance and breach of rights to privacy and correspondence. In addition, the court ruled that data retention from a perspective of crime fighting is too vague and generalized.[44]

The judgment instilled the principle that vague rules cannot be applied, and sufficient safeguards must exist on the national level, prompting Member States to revise their data retention rules. Based on this ruling it is evident that in the event of the invalidation of the Directive the individual Member States were left on their own in terms of clearing up the legal inconsistencies, and although some States have been diligent in this regard, improving or rewriting the old legislation, the others have not been so successful. The following chapter takes a closer look at the current state of national data retention legislation in order to determine if the subsequent efforts to harmonize data retention laws across the European Union have improved over the last 6 years, since the invalidation of the Data Retention Directive.

[42]OJ L 201, 31.7.2002.

[43] Judgment, 21.12.2016, C-203/15 & C-698/15, EU:C:2016:970, *supra nota* 40.

[44]Rauhofer, J., Sithigh, D. (2014). The Data Retention Directive Never Existed. *A Journal of Law, Technology and Society*, 11(1), 123.

2.2. Data Retention Regimes in the European Union After the Invalidation of the Data Retention Directive

The Telecom sector regulations concerning data retention lack coherence, which is evident by the difference in national laws in different Member States. In addition to inconsistencies being caused by a lack of coherent scope, after the invalidation of the Data Retention Directive the Member States already had varying levels of implementation of the Directive which was not harmonized after the invalidation.

Estonia, for example, implemented the Data Retention Directive into the Estonian Electronic Communications Act, whereby the law states that retention of information applies to non-anonymous telephone and Internet data, which must be held for a year from the date of communication.[45] Germany and Romania national courts ruled the law transposing the Directive lacking in defined scope, too ambiguous and lacking safeguards for access and handling or retained data, while Cyprus and Lithuania courts declared the law implementing the Directive unconstitutional[46]. On the other hand, the United Kingdom has created its own Data Retention and Acquisition Regulations[47] which gives more defined safeguards as to when, how and by whom the data can be retained and accessed, but its approach is more of an exception than a rule. Similarly, Germany and Belgium have created their own laws on data retention, whereby Germany has specifically made data retention law on the basis of CJEU findings and decision of Digital Rights Ireland.[48]

In conclusion, based on the examination of different legal systems, European Union Member States have all varying data retention laws, thus lacking cohesion, therefore being in need of harmonization of law on national level. This finding furthermore supports the posed hypothesis that the data retention regime in the electronic communications sector needs reform. Where some States like Germany and Belgium have been more diligent in creating new laws and implementing CJEU findings in mind, other States still have a lot of work to be done.

---

[45] RT I, 01.01.2005, §111(2,4).
[46] Munir, Yasin., Bakar (2017), *supra nota* 31, 74.
[47] Data Retention and Acquisition Regulations, 31 October 2018. Article 8. Accessible: https://www.legislation.gov.uk/uksi/2018/1123/pdfs/uksi_20181123_en.pdf
[48] Munir, Yasin., Bakar (2017), *supra nota* 34, 76.

2.3. E-Privacy Directive data retention principles

Efforts have been made to bring forth more concise legal instruments in order to address the issues the Data Retention Directive and its invalidation had created. The e-Privacy Directive 2002/58 was passed in 2002, amending previous data retention Directive 97/66/EC and staying as a general guideline for States in data retention questions. The Directive also defined data retention as a measure to detect, prevent and prosecute criminal offences, which set ground to Member States having Telecom sector service providers invest in equipment designed to retain large amounts of data to comply with the Directive, although not all providers agreed to do it. [49]

After the invalidation of the Data Retention Directive, the ePrivacy Directive article 15(1) served as a provision for determining how data in the European Union Telecom sector was protected, accessed and used. Although the Directive laid out provisions to protect the privacy of electronic communication users, it did not define, same as the invalidated Data Retention Directive, the term 'serious crime' and exhibited the same issues the invalidated Directive had.[50] In addition, the e-Privacy Directive allowed restrictions for the prevention, detection, investigation and prosecution of any criminal offence, making the Directive difficult to transpose into practice[51].

The e-Privacy Directive might have helped the Member States on a national level by providing more concise provision on safeguards in protecting data privacy at the time, but it was data retention for criminal investigations where the Directive was lacking. When the Data Retention Directive was invalidated the e-Privacy Directive was not amended to fill the existing legal gaps.

2.4. European Electronic Communications Code

The upcoming new legislation called the European Electronic Communications Code (EECC) is set to come into force by December 2020 and is aiming to address some of the issues that were present in previous legislations.

---

[49] Dusanovic (2010), *supra nota* 22, 45.

[50] 13.Calomme, C. (2016). Strict Safeguards to Restrict General Data Retention Obligations Imposed by the Member States. *European Data Protection Law Review*, 2 (4), 594.

[51] *Ibid*.

Upon analysing the Directive, it is evident that it has managed to bring together old and new electronic communication methods under the same umbrella definition,[52] adding the methods of new business models relying on the internet for delivery within its scope. This means that the new technological advancements in communications abide by the same rules as the traditional Telecom sector methods. This is a big step towards harmonization of the legal framework as it allows to regulate the services equally at the same time.

On the other hand, the Directive does not once mention data retention, which means the question of harmonizing data retention rules across the European Union have not been taken on in this instrument. This still leaves the States to individually manage data retention rules solely on the basis of the national law and the CJEU recommendations.

[52] OJ L 321, 17.12.2018, article 2.

3. LEGAL CHALLENGES CONCERNING ADOPTION OF NEW DATA RETENTION REGULATION IN THE EUROPEAN UNION TELECOMMUNICATIONS SECTOR

In this chapter the legal gaps are assessed and organized, based on the existing principles discussed in previous chapters. Scope of data retention is defined, questions asked about what needs to be considered before any new legislation can be made. Having gathered relevant information about past and current legal frameworks concerning data retention in Telecom sector, analysis on a possible new legislation can begin.

3.1 Irregularities in national laws

The first legal gap, as identified in the previous chapter, is the non-unified transposition of the failed Data Retention Directive into national law of each Member State. Where some Member States transposed the Directive almost fully, others created new laws altogether, which created a situation where instead of harmonized laws throughout the European Union, the transposition of laws has had the opposite effect. This poses problem of gathering data in cross-border investigation cases, whereby in States data is not available by national law in one country will hinder the investigation in another, for example. This problem serves as an evidence of needing to introduce a cohesive, Union-wide framework that can be transposed into the national law of each Member State in the same manner as the TFEU is - by having a cohesive framework throughout, the issues regarding implementation data retention laws will help to bring equal legal form into all States.

3.2. Data retention and privacy

According to the Data Retention Directive, data retention means the preservation of traffic and location[53] and data necessary to identify the registered user[54] in order to be able to assist with criminal investigations, as data retention could provide essential digital evidence for prosecution

[53] OJ L 105, 13.4.2006, article 1 (2).
[54] *Ibid.*

in a criminal matter. The data showing the content of the communication is not permitted to retain[55], however, a lot of the time a location data can reveal a lot more about the person than necessary, considering it can show patterns of behaviour, comings and goings of the person and who they interact with.[56]

As discussed in previous chapters, there is a constant balancing act between a person's privacy and security warranting the breach of privacy. One of the bigger efforts the European Union has made is introducing the General Data Protection Regulation in 2018. The regulation mainly focuses on protection of data and limiting its processing by data controllers.
Although it has been a more positive push for individual privacy protection, it has also highlighted an issue with data retention - the GDPR allows gathering data for statistical purposes only by anonymizing it.[57] Moreover, the GDPR does not allow processing of data for any reason except for the primary reason it was requested for,[58] making gathering data in the Telecom sector more difficult, if it was to be governed only by GDPR.
This means, in order to have a successful data retention for the purpose of criminal investigations, the proposed legislation should only govern Telecom sector specifically and be justifiable to override GDPR data retention restrictions within the sector, while still keeping in mind protection of individual privacy, which can be achieved by principle of proportionality.

3.3. Data retention and proportionality

Besides considering a person's privacy from human rights perspective, data retention laws also need to pass the proportionality criteria, as mandated by CJEU during the Digital Rights Ireland case. According to the Human Rights Charter, interference with privacy can be justified in certain cases, which the Court outlined in the judgment of the case. The proportionality test requires the legislation to pass four criteria: 1) Definition of scope of the purpose; 2) transparency; 3) proportional data security standards and 4) effective legal remedies including sufficient judicial control[59].

---

[55] *Ibid*, article 5 (2).
[56] Dusanovic (2010), *supra nota* 21, 46.
[57] 14.Mayer-Schonberger, V.; Padova, Y. (2016). Regime Change: Enabling Big Data through Europe's New Data Protection Regulation. *Columbia Science and Technology Law Review*, 17 (2), 322.
[58] *Ibid*.
[59] Vedaschi, Lubello (2015), *supra nota* 34, 26.

First, as observed in the Data Retention Directive analysis, the directive failed to define the scope of the purpose sufficiently by omitting data retention and serious crime definition. In order for the legislation to work, it needs to be precise in defining what is the purpose of the retained data- detection, prevention, investigation and prosecution of crime - as well as defining what crime falls into the scope of the legislation. The ongoing case in Estonian court C-746/18 outlined the problem at hand with lack of definition in the data retention, which in turn is raising an important question in the case - does the law enforcement have the right to request access to communications data of a person who has committed a minor offence.[60] Because the Court mandated that the seriousness of a crime needs to correlate proportionately to the way the private data is handled, it will vary between the States, as the interpretation of ''serious crime'' has been left to their discretion. If the data is retained with the purpose of prosecuting crime, it is serving the correct purpose and the next step should be to define what category of crime the data retention should help to prosecute and whether it would be proportionate to the type of data access required to solve a specific crime.

Furthermore, knowing the concerns around a general blanket data retention obligation, there should be clearly defined limitations as to whose data can and cannot be retained. By that, persons in particular need for professional secrecy and persons under protection could be excluded. From the Court's findings it is evident that blanked data retention rules should not exist in the future regulation and with the help of technology the exclusion of retaining certain person's data should be possible.

Second, transparency within the legislation needs to be present not only for reassuring the public that their privacy is respected but also to limit the unauthorized and improper access to individuals' data. The Court has expressed that it has not been clear who specifically is allowed to access the data. It is also unclear what kind of safeguards are in place to ensure the data can only be accessed lawfully and through a specific procedure that can prevent misuse of the system. Should there be an unlawful access or use of retained data, a procedure for dealing with such breaches needs to be outlined as well, placing the accountability not only on the service providers but also on the competent authorities who have access to such data. The specific period the data is retained needs to be reassessed. This also means that the service providers need to be held to a higher security standard and not be only doing the minimum in terms of safeguards.

[60] Opinion, 21.01.2020, C-746/18, EU:C:2020:18.

Third, the principle of proportionality in this context requires that the level of crime committed corresponds to the extent of the interference with privacy. The service providers cannot collect such enormous amounts of personal data just in case, but if it's not yet technologically possible to exclude certain data from being retained, then the access clearance to the retained data should be significantly harder to obtain, both from authorized parties and unauthorized individuals and other entities. In order for this to be possible, the rules laid down must be as precise as possible, in order to be able to justify such an extensive and all-encompassing collection of individuals data at all.[61]

Fourth, the effective legal controls and remedies need to be in place in case there is an unauthorized or arbitrary access and misuse of the retained data. So far there has been little evidence of oversight in regard to procedures on how data is being accessed and logs to know who and for what purpose has accessed a person's retained data. The absence of effective oversight leads to lack of transparency and control of data access. Such lack of control also puts people's privacy at risk because there is no way to know who has accessed their information and for what purposes, which invites potentially harmful persons or organizations having access to people's data without any record-keeping or remedy in case the information is used against the person in an unlawful way.

According to the Treaty of the Functioning of the European Union article 85(1), the EU should promote and support the creation of measures that aid in criminal investigations and prosecutions, inside the Member States and cross-border. This has already been implemented in the Financial sector in terms of securing an AML regulatory framework. As the Telecom sector is also one of the industries where data collection can aid in crime prevention, investigation and prosecution, there is reasonable expectation for the Telecom sector to follow suit in a similar manner.

[61] Eisendle (2014), *supra nota* 25, 458.

4. DATA RETENTION LAWS IN FINANCIAL SECTOR- JUSTIFIED RULES FOR INTERFERENCE WITH PRIVACY

The financial sector is regulated by the sector's regulators such as the Financial Task Force (FCA) in the United Kingdom, Finantsinspektsioon in Estonia and the European Banking Authority (EBA). The European Union adheres to the 5th Money Laundering Directive,[62] which outlines the measures which financial institutions need to implement in order to fight crime, fraud and AML/TF. Unlike electronic communications service providers, a financial institution cannot provide its services without a regulator's approval for a licence in the region. Thus, all financial institutions must adhere to the regulations concerning anti-money laundering and terrorist financing (AML/TF). The financial institutions themselves are private companies with their own set of terms and conditions each person signs when they become a customer of that service provider and it is their responsibility to make sure they are in line with the AML/TF regulations and conduct due diligence on their customers prior to beginning of the business relationship and during it.[63]

It is up to the regulators to agree on specific recommendations and compile them into an actionable documentation, such as what the Financial Action Task Force (FATF)[64] has done. The aim of FATF is to set an international standard in terms of combating money laundering and terrorism.[65] This warrants a specific process to be devised, whereby all concerned parties (regulators and service providers) know and follow rules that are interpreted similarly in all Member States.

Each financial institution is required to have a policy on their Know-Your-Customer (KYC) measures, meaning they have to conduct checks on their customers, from the beginning of the business relationship when the customer agrees to their terms of use, to periodical checks and extra questions regarding transfer of funds[66]. Financial sector has essentially the same obligation as the

---

[62] OJ L 156, 19.6.2018.

[63] Böszörmenyi, J., Schweighofer, E. (2015). A review of tools to comply with the Fourth EU anti-money laundering directive. *International Review of Law, Computers & Technology*, 29 (1), 67.

[64] International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Accessible: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html June 2019.

[65] Böszörmenyi, Schweighofer (2015), *supra nota* 63, 64.

[66] Standard documentation requirements that are required of the service providers in the sector. Based on internal documentation of TransferWise Ltd.

Telecom sector to retain customer data and sets the obligation to transpose data retention from AML/TF regulations directly on the financial institutions processes. When comparing the two sectors it must be noted that while the purpose of data retention is to fight crime in both sectors, they still have significant differences in what kind of crime the data is mainly being used for. Because the financial sector deals with money-related crime, the data it gathers is fundamentally different - it would not be possible to retain the same kind of financial data in the Telecom sector. Data must be retained in the financial sector because it enables the law enforcement to prevent, detect, investigate and prosecute crime. There are several types of crimes that can be solved with data retained - economic crimes such as serious fraud, money-laundering, financing terrorist organizations either directly or indirectly, trafficking, cybercrimes, identity theft, economic abuse and others.[67] The nature of the sector is that it allows would-be customers to sign up on the condition that a certain amount of data is collected and verified against evidence[68] (verifying identity by providing identification documentation, for example). By signing up to use a service the customer is informed that they agree to adhere to AML/TF related inquiries, should there be a need. Many such services have provisions in their terms of use clause that state the necessity to process such data during and after the business relationship in order to comply with regulations.[69]

The obligation concerning data retention for combating crime is put on the service providers directly and supervised by the financial regulators. This creates a system where the financial institution is subject to regular checks or audits to make sure the regulations have been not only properly implemented but also practiced in reality. Therefore, the Financial sector has a specific authority looking after the proper implementation and practice of regulations, whereby failure to comply with is punishable by fines or loss of licence to provide services.

The regulations are allowed to interfere with privacy of the consumer because this sector is combatting financial crime and terrorism - money laundering can be classified under ‘’serious crime’’ and fighting terrorism is in the public interest, as confirmed in the Digital Rights Ireland case law, thus being justified under the Charter of Fundamental Rights article 8.[70] Therefore, justification to look into a person’s personal data transaction history or fiscal patterns is

---

[67] Böszörmenyi, Schweighofer (2015), *supra nota* 63, 64.

[68] 17.Shehu, A. (2010). Promoting financial sector stability through an effective AML/CFT regime. *Journal of Money Laundering Control*, 13, 143.

[69] TransferWise Europe outlines data retention obligations. Privacy policy section 9. Accessible: https://transferwise.com/privacy-policy-tw-europe

[70] Böszörmenyi, Schweighofer (2015), *supra nota* 63, 72.

proportional in these cases as it has a proven track record of combatting this type of crime. Without the use of this retained data it would not be possible to prevent and investigate such crimes.

4.1. Retaining Data for Criminal Investigation in Financial Sector

For the purposes of understanding how the data retention in the Financial sector works, analysis of the main AML/TF legal instrument in the European Union, the 5th AML Directive, is needed. The 5th AML Directive aims to respect person's privacy and at the same time observe and apply the proportionality principle in its data retention methods.[71] It argues that anonymity increases the risk related to crimes being committed as it protects the individuals from the law enforcement.[72] Therefore, the Directive justifies that it is necessary to gather non-anonymized data for purposes of battling crime, as long as it is done in a proportional way. In order to collect data while respecting privacy the Directive proposes to only collect minimal amounts of data necessary and hold it in centralized automated mechanisms.[73] The data is retained for a minimum of 5 years and can be retained for 5 more for investigation purposes, depending on the situation.[74]

The Directive also makes a distinction between different types of customers and requires monitoring them on a risk-based approach.[75] While it is unnecessary in the Telecom sector as there is no economic matter to protect, the Financial sector has made a good distinction of who is a higher risk consumer and how they should be monitored. However, the Directive makes a point of creating a proportionate approach in order to guarantee privacy rights by having Member States to not have to ask of certain individuals information with the help of special registers, as having their data exposed may put that person put in danger of being harassed, extorted, kidnapped or blackmailed among others.[76]

The Directive puts an obligation on the financial services providers to collect a certain kind of data. Unlike the Telecom sector, where only subscriber and traffic data is linked and collected, the

[71] OJ L 156, 19.6.2018, preamble (5).
[72] *Ibid*, preamble (9).
[73] *Ibid*, preamble (21).
[74] *Ibid*, preamble (44).
[75] *Ibid*, preamble (24).
[76] *Ibid*, preamble (36).

financial sector must collect and verify sufficient data in order to be able to identify the customer.[77] In the case of fighting financial crime, the financial sector must collect more data than other sectors, in order to be able to analyse the data and patterns that help with building crime-preventing and detecting systems. Because the data is gathered at the beginning of the business relationship between a customer and the service provider, oftentimes it means that data is gathered upfront and then through monitoring payment patterns, as the person is moving money from one account to another, this data is gathered and analysed as well. This means the data retention and processing is done continuously, in addition to having it available for the law enforcement to access, if needed. Moreover, the amount of data collected depends on the risk-based approach each financial institution has taken, meaning some institutions may ask for more information from certain customers than other institutions, thus having more data retained.

The access to retained data by outside parties is more strictly regulated as well. The Directive calls for Member States to put in place specific safeguard to ensure the data retained is accessed only by authorized entities by placing an independent supervisory entity to manage it[78]. This creates a network of entities who can have access to such data, such as the public authorities in the State and cross-border law enforcement. By having this specialised overseeing entity ensure compliance of data retention and access it is easier to place safeguards and monitor access, than leaving it only into the hands of the service providers to make choices. Moreover, the financial sector also has a remedy system, whereby the service user can file a complaint to a competent authority called the Ombudsman who can review customers complaints and issue a remedy for breach of terms of use or any mishandling of customer's information.[79]

The analysis shows that the financial sector has thought of data retention in more detail and has placed strict but effective safeguards in order to be able to use the data retained without compromising on data protection or proportionality. The points brought up in this chapter will serve as a comparison with the current Telecom principles and will be analysed in the context of bringing over possible solutions from the financial sector legislation to the potential Telecom legislation.

---

[77] OJ L 141, 5.6.2015, Article 13.
[78] OJ L 156, 19.6.2018, preamble (44-45).
[79] Financial ombudsman listed on TransferWise website. Accessible: https://transferwise.com/help/24/technical-issues/2235393/customer-complaints-procedure

5. PROPOSED LEGISLATION FOR TELECOMMUNICATIONS SECTOR ON THE BASIS OF FINANCIAL SECTOR LEGISLATION

Based on the findings of the previous chapter there are quite a few recommendations that can be made for the purpose of closing the legal gaps found in the second chapter and creating a new data retention regime for the Telecom sector in the EU. It is evident that the Financial sector regulatory framework relies a lot on regulators in each Member State, whose purpose is to uphold the proper transposition and practice of financial regulations and directives, however they are all in harmony because of the overarching 5th AML Directive that guides all Member States financial service providers and their regulators who impose the laws in an efficient manner, as well as regulators and FATF who oversees that the standards are met. The first proposal, therefore, is to have a Telecom regulator tasked with similar, if not the same kind of purpose, in order to make sure the correct interpretation and implementation of data retention laws is upheld.

Second, data retention legislation must have universally understood definitions and scope across all Member States concerning 1) data retention, including what type of data will be retained;
2) serious crime definition and whether other types of crimes or misdemeanours also fall under the scope of the legislation; 3) how long is specific data retained and whether exceptions are allowed. The main issue to solve is whether the privacy of a suspect can be waived in favour of prosecuting them of the crime the law enforcement has enough reason to suspect them of. The proportionality of solving crime in this instance should be examined further and weigh the suspect's privacy against the possible successful crime solving.

One of the cornerstones of the data retention regime in the financial sector is the verification of person's identity and authentication of customers. While provision and consumption of financial services should not be possible anonymously, and this core rule cannot directly cross-over from one sector to another, a differentiated approach based on personal identification and authentication in the electronic communications sector may be conceivable. As it is an accepted trade-off in financial services that a customer wishing to use the services of a financial institution accepts certain data retention rules and hence interference with privacy, in a trade-off in the context of electronic communications a customer willing to verifiably identify and authenticate for the use of

services should enjoy more privacy in the form of limited data collection. While the less reliably identified and anonymous users' communications may remain subject to blanket data retention rules. Arguably personal identification in the use of electronic communications services could make it practically possible to differentiate between data subjects, devise proportionate rules where possible and limit data retention at the collection phase according to the Tele2 judgment. While this solution raises a sea of new questions, the existing legislative framework under the eIDas[80] Regulation may make this a feasible option in the EU.

Third, there needs to be a procedure for accessing retained data. The proportionality principle must be upheld when accessing retained data, meaning only authorised persons are able to access data on a basis where it has been proven that there is sufficient evidence to support the person is a suspect in a crime. No data should be accessed proactively or without proof. Although the nature of the Financial sector provides a reasoning for accessing and processing persons data proactively by the service providers, the same method cannot be used in the Telecom sector due to the nature of the sector's data. However, it should be re-examined which crimes or misdemeanours warrant comprehensive access to a specific subject's data by the law enforcement. For the data to be available for law enforcement purposes there needs to be an oversight of how data is accessed and managed. This can be done by implementing the Police Directive principles, whereby there is an overview of data handling as well as data subjects being notified who and why is accessing their data. Thus, each request and successful access need to be documented. The Police Directive could serve as a basis on which Telecom data retention and processing by competent authorities is transposed into national legislation and the data processing authorities are bound by law to use data in authorised and lawful manner.

By the financial sector's example, in order to respect the privacy of certain individuals who should be protected more from such access, there should be exceptions to retaining data of vulnerable persons or those with professional confidentiality. Similarly to the Financial sector, there needs to be an Ombudsman-type complaint body where data subjects can direct their objections to how their data is used. This ensures that cases where data subjects rights are being violated can be effectively solved and remedied through appropriate channels. Such method could provide more transparency to how the subject's retained data is used.

[80] OJ L 257, 28.8.2014, p. 73–114

Lastly, author recommends applying similar international co-operation standards to Telecom sector as there are in the financial sector. By having an effective and constant feedback, training and aid between Member States, solving cross-border crimes can become quicker and more efficient. In regard to data security standards, it is paramount that the effort of creating good security standards should be upheld. It should be discussed in more detail whether development of such security measures should be put on service providers or whether the regulator or independent parties could be tasked with developing tools to guard the retained data in best possible ways. There should be no option of having a new policy created with data retention having minimum security standards.

CONCLUSION

Technology is all around us. Majority of humans use phones and the Internet daily, creating vast amounts of personal data that gets retained, from a message on Facebook to a phone call to a friend. The retained information is the most important piece of data that can be used as evidence in criminal investigations, because everyone leaves a trace online or via telephone communication services. Naturally, the law enforcement has the potential to prevent and solve crimes more easily if they have access to such data. However, we also live in a world where privacy and protection of our data is becoming more and more important. The struggle between privacy and security is a tight balancing act which policymakers need to have in mind when regulating the Telecom sector.

The aim of this thesis was to provide suitable recommendations for the Telecom sector data retention legislation policy makers by analysing the gaps of Telecom sector's policies and comparing two sectors that retain data for the purpose of criminal investigations - the struggling Telecom sector and the strictly and efficiently regulated Financial sector. The hypothesis was created as such: the Telecom sector's data retention laws should be reformed. Data retention principles in the Financial sector could serve as a basis to fill the legal gaps, serving as a proposal of ideas for new legislation for policy makers looking to improve upon the Telecom sector principles.

The author first analysed the Telecom legislation concerning data retention in detail, finding a set of principles that should be present in a successful data retention legislation. Issues with the current framework were discussed. The legal gaps concern mainly the Telecom sector's inability to balance individual's privacy with proportionality. The previous legislation concerning data retention have not provided definitive solutions to the proportionality issue, however they showed specific issues that should be fixed, providing the author with legal gaps that need to be addressed. Issues such as lack of oversight, transparency and process were identified, as well as the issue that blanket data retention rules cannot be applied as an excuse to prevent crime. The CJEU provided four criteria to consider when checking proportionality of the law, definition of scope of the purpose, transparency, proportional data security standards and effective legal remedies, which could be used as a basis of building a new policy in principle.

Next, the author analysed the Financial sector data retention laws and determined what criteria makes the sectors principles effective and proportionate. The Financial sector is more structured, mainly because of the fiscal nature of the sector. The proportionality principle works better in the sector, because it combats serious crime such as money laundering and terrorist financing. The power to regulate and audit the service providers is also constructed in a way that the service providers can be held accountable for their data handling.

The two sectors' principles were then collected and compared with one another, resulting in the author answering the main question that financial sector's data retention principles can be used to help close the legal gaps of Telecom sector's data retention policies. Thus, the recommendations for the Telecom sectors were provided in the last chapter. The Telecom sector could implement several principles in the new policy, such as having a more comprehensive logic of who's data should be accessed and by whom, having an independent body regulating the sector and providing enough confidence to data subjects in cases of unauthorized data access or misuse. The sector should have a process in place that is well thought through and holds all parties accountable for data retention and access for criminal investigation purposes. In addition, the creation of better cooperation between Member States in terms of cross-border crime investigation and research of new methods of retaining data securely would be recommended.

The author recommends, for further research, to continue expanding on proportionality within technology-heavy sectors and draw parallels in researching them, in order to compare and create new ideas on how to keep security and privacy equally balanced when creating legislation on data retention for criminal investigations.

LIST OF REFERENCES

Scientific books:

1. Black, S. (2001). *Telecommunications Law in the Internet Age*. USA: Elsevier Science & Technology.
2. Graig, P., De Burca, G. (2015). *EU Law: Text, Cases, and Materials*. (6th ed.) United Kingdom: Oxford Press.
3. T-E. Synodinou, P. Jougleux, C. Markou, T. Prastitou. (2017). *EU Internet Law: Regulation and Enforcement.* Switzerland: Springer.

4. **Scientific articles:**

5. Borgesius, F.J.Z., Steenbruggen, W. (2018). The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust. *Theoretical Inquiries in Law, Forthcoming*, 19 (2), 291-322.
6. Bignami, F. (2007) Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law*, 8 (1), 233-255.
7. Breyer, P. (2005) Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. *European Law Journal*, 11(3), 365-376.
8. Brown, I. (2010). Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology*, 19 (2), 95-109.
9. Brown, I., & Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology*, 6 (2), 119–134.
10. Böszörmenyi, J., Schweighofer, E. (2015). A review of tools to comply with the Fourth EU anti-money laundering directive. *International Review of Law, Computers & Technology*, 29 (1), 63-77.
11. Calomme, C. (2016). Strict Safeguards to Restrict General Data Retention Obligations Imposed by the Member States. *European Data Protection Law Review*, 2 (4), 590-595.
12. Dusanovic, D. (2014). Implications of Invalidity of Data Retention Directive to Telecom Operators. *Juridical Tribune*, Vol. 4 (2), 43-59.

13. Eisendle, D. (2014). Data Retention: Directive Invalid - Limits Imposed by the Principle of Proportionality Exceeded. *Vienna Journal on International Constitutional Law / ICL Journal*, 8 (4), 458-461.
14. Feiler, L. (2010). The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. *European Journal of Law and Technology*, 1 (3).
15. Friedewald, M., Pohoryles, J. (2013). Technology and privacy. Innovation. *The European Journal of Social Science Research*, 26, 1–6.
16. Mayer-Schonberger, V.; Padova, Y. (2016). Regime Change: Enabling Big Data through Europe's New Data Protection Regulation. *Columbia Science and Technology Law Review*, 17 (2), 315-335.
17. Munir, A.B., Yasin, S.H.M., Bakar, S.S.A. (2017). Data Retention Rules: A Dead End. *European Data Protection Law Review*, 3 (1), 71-83.
18. Rauhofer, J., Sithigh, D. (2014). The Data Retention Directive Never Existed. *A Journal of Law, Technology and Society*, 11(1), 118-127.
19. Shehu, A. (2010). Promoting financial sector stability through an effective AML/CFT regime. *Journal of Money Laundering Control*, 13, 139-154.
20. Vedaschi, A., Lubello, V. (2015). Data Retention and Its Implications for the Fundamental Right to Privacy. *Tilburg Law Review (Gaunt)*, 20 (1), 14-34.
21. Warken, C., Zvieten, van L., Svantesson, D. (2019). Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence. *International Review of Law, Computers and Technology*, 34 (1), 44-64.

Estonian Legislation:

22. Estonian Electronic Communications Act. RT I, 01.01.2005.

EU and international legislation:

23. European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.
24. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002.

25. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, 37-47.
26. 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, OJ L 105, 13.4.2006, 54–63.
27. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.
28. Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds, OJ L 141, 5.6.2015, 1–18.
29. European Parliament and of the Council of 20 May 2015 Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73–117)
30. Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, OJ L 337, 23.12.2015, 35–127.
    Directive 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, 43–74.
31. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, 36–214.
32. Data Retention and Acquisition Regulations, 2018, 1123.
33. ETS. 185 Budapest Convention on Cybercrime .

Court decisions:

34. CJEU, Case C-293/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others [2014]
35. CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen, Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis [2016]
36. CJEU, Case C-746/18, K.H v Prokuratuur [2020]

Web materials:

37. European Union Agency for Human Rights. Accessible: https://fra.europa.eu/en/publication/2017/data-retention-across-eu July 2017.
38. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Accessible: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html June 2019.
39. Constitution of the International Telecommunication Union, Annex, p. 65. Accessible: https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx

Appendix 1. Non-exclusive licence

Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I, Kristina Rutšjevskaja,

1.Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

Telecommunications Data Retention Regulations and Criminal Investigations – Solutions from the Financial Sector,

supervised by Agnes Kasper, PhD,

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*