RIGA GRADUATE SCHOOL OF LAW

Electronic Communications Law legal issues and the effect of it towards freedom, security and justice in the Republic of Latvia

MASTER'S THESIS

AUTHOR: Elvīra Cupika

LL.M 2019/2020 year student

student number M019049

SUPERVISOR: Inguss Kalniņš

Mg. sc. soc.

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed) …….

RIGA, 2020

ABSTRACT

On 15 March 2006, the European Union adopted the Data Retention Directive 2006/24/EC[1] which regulated the Internet Service Providers storage of telecommunications data and could be used to fight serious crime in the European Union. This directive was needed, because people in the European Union needed a higher level of data protection. Since multiple countries had their own data retention laws, the European Parliament and the Council saw the need to harmonise and strengthen the data retention in the European Union. Despite the noble intentions, the European Court of Justice declared it invalid on 8 April 2014.[2] Yet, the essence of the Directive was transposed to each and every national data retention law across European Union. In this master thesis, author examines whether member states, but particularly, The Republic of Latvia has learned anything from the invalidation of the Directive 2006/24/EC. The author of this thesis will first of all, look into the adoption and invalidation reasons of the Directive 2006/24/EC. Following that the author will look into the to see if there is any resemblance to the Directive 2006/EC/24, considering the fact that this law consist of norms that are directly transposed from the Directive 2006/24/EC. In order to conclude whether the Electronic Communications Law is affecting the freedom, security and justice in Latvia, author will analyse whether the arguments presented by the European Court of Justice are applicable to the Electronic Communications Law[3].

Keywords: Data Retention; Electronic Communications; Telecommunication; Digital Rights Ireland; European Court of Justice; Right to Privacy; Data protection; The Directive 2006/24/EC.

[1] European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.
[2] Judgment of the Court (Grand Chamber), 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Available on: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN Accessed April 2, 2020.
[3] Latvijas Vēstnesis. Elektronisko sakaru likums, 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed March 30, 2020.

SUMMARRY

On 1 May 2004 Latvia joined the European Union. As a member state, Latvia had to implement multiple directives into its national legislation. In this master thesis, author focused on the Directive 2006/24/EC, that upon adoption had to be incorporated into the Electronic Communications Law. This directive was transposed by all member states of the European Union in order to harmonise data retention laws within the European Union. Even though this directive was considered a controversial, countries did not hesitate to transpose the legal norms of the directive into their national laws.

The same controversial questions were raised again, six years after the directive was adopted. This time, those questions came from Ireland and Austria and were submitted to the European Court of Justice. The final judgement of the case *Digital Rights Ireland* became one of the most known judgements in the field of the fundamental human rights. In this judgement the European Court of Justice analysed the compatibility of the European Union's legislation with the fundamental human rights. This judgement has strengthened the fundamental human rights in the European Union.[4]

Despite the argumentation of the European Court of Justices, not all member states learned from the mistakes of the past. To this day, there are still a few member states that has some part of the Directive 2006/24/EC included in their national laws. One of those member states is Latvia. The Electronic Communications Law, even with the recent amendments, the Electronic Communications Law have more than just a few legal norms of the Directive 2006/24/EC left.[5]

In order to test whether the Electronic Communications Law is violating the fundamental rights just like the Directive 2006/24/EC, the author explained the history and issues of the Directive 2006/24/EC. To understand the issue at hand, author explained the importance of the right to privacy and protection of personal data. Further, the validity of the Electronic Communications

[4] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 08 April 2014. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 . Accessed on May 9, 2020.

[5] Elektronisko sakaru likums. Latvijas Vēstnesis, 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed March 22, 2020,

Law was tested by applying the same arguments that were presented by the European Court of Justice.[6]

Since this master thesis was written during the pandemic, author did a research on whether the new regulation affecting fundamental rights. New regulations were adopted in order to combat the COVID-19. Author saw this new regulation interesting, because it authorised another institution to have access to a personal data.

This research is the first step towards a greater discussion. Unlike the other countries of the European Union, Latvia has chosen to stay silent on this topic. This is the first ever written research, that is questioning the validity of the Electronic Communications Law. To raise some sort of discussions, the author has submitted three questions to two state authorities and after receiving the answers, the author evaluated, whether those answers can hold up to the critique. It is important to raise an awareness of possible human rights or other right violation. However, the authors aim is to have this discussion to make the national legal system a better place, to improve it. Lawyers and other researchers tend to attack legislators or other state institutions if they find the smallest defect in our legal system. This master thesis consists of critique towards legislator of Latvia, but it is there to highlight the serious issues that the Electronic Communications Law is causing towards freedom, security, and justice in the Republic of Latvia.

[6] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 08 April 2014. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 . Accessed on May 9, 2020

TABLE OF CONTENTS

Introduction

Modern world and global society is challenging legislators around the world.[7] Ever since people started using social media platforms, online stores and other possibilities that the internet gave us, became a challenge for legislators have been challenged on national and international level, because they have to come up with laws that would keep up with ever-growing electronic communications and find new ways how to safeguard people's rights.[8]

In the past twenty years, there have been plenty of laws that were trying to find the perfect balance between obtaining data for state security reasons and safeguarding fundamental human rights.[9] In 2019 my attention was brought to European Union's Directive 2006/24/EC[10] because it seemed like a great tool for data related issue regulation. The Data Retention Directive[11] also laid out the foundation for multiple member state's national data retention laws that were invoked right after the Data Retention Directive came into force.[12]

The Data Retention Directive helped to solve multiple criminal cases that included combatting terrorism, but it was not designed in a way to combat only criminal activities around European Union, this caused multiple controversial discussions.[13]

Firstly, in this thesis I will discuss why Data Retention Directive[14] was announced to be invalid[15] by the European Court of Justice and which fundamental rights that were breached were

---

[7] Marcin Betkier. Privacy Online, Law and the Effective Regulation of Online Services, pp. 79-100. Intersentia, Cambridge, Antwerp, Chicago, 2019.

[8] Anabela Susana De Sousa Goncalves, "Extraterritorial Application of the EU Directive on Data Protection, The," Spanish Yearbook of International Law 19 (2015): 195-210 Available on: https://heinonline.org/HOL/P?h=hein.intyb/spanyb0019&i=195. Accessed 02.04.2020.

[9] European Parliament and European Council. Directive 95/46/EC. Available on: https://europa.eu/!Xb76Xu . Accessed on April 14, 2020. European Parliament and European Council. Directive 2002/58/EC. Available on: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 Accessed April 9, 2020.; European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[10] European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[11] Ibid.

[12] Library of Congress. European Union: ECJ Invalidates Data Retention Directive. Available on: https://www.loc.gov/law/help/eu-data-retention-directive/eu.php Accessed April 11, 2020.

[13] Report from the Commission to the Council and the European Parliament. Evaluation report on the Data Retention Directive. Available on: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A52011DC0225%3AEN%3AHTML Accessed April 14, 2020.

in the opinion of the European Court of Justice.[16] Since the Directive 2006/24/EC was transposed to multiple national laws in Europe, I examined what happened to those laws after this directive lost its powers, by researching case law of countries like Germany[17], Ireland[18]and Hungary[19], where courts declared that national laws are breaching the fundamental right to privacy.

Secondly, I researched whether the Latvian national Electronic Communications Law[20], that is implemented[21] on the grounds of the Data Retention Directive 2006/24/EC[22] can be considered lawful.[23] In order to do so, I analysed existing case law in order to find out how other countries dealt with this issue and compared the Electronic Communications Law[24] with the Directive 2006/24/EC[25]. Further, I applied the proportionality test that helped to find out whether this law

---

[14] European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[15] Judgment of the Court (Grand Chamber), 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Available on: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN Accessed April 2, 2020.

[16]Council of Europe. European Convention on Human Rights, Article 8. Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf. Accessed March 4, 2020; The European Parliament. Charter of Fundamental Rights of the European Union, Article 7. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed March 15, 2020.

[17]European Court of Human Rights, Weber and Saravia v. Germany, June 29, 2006. Available: http://hudoc.echr.coe.int/fre?i=001-76586 Accessed April 7, 2020.

[18] Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v. Data Protection Commissioner. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 Accessed April 3, 2020.

[19] European Court of Human Rights. Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016. Available on: https://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf Accessed April 10, 2020.

[20] Saeima. Grozījumi Elektronisko sakaru likumā. Latvijas Vēstnesis, 21, 30.01.2020. Available on: https://likumi.lv/ta/id/312285 . Accessed April 11, 2020.

[21] 2007. gada 3. maija likums "Grozījumi Elektronisko sakaru likumā". Latvijas Vēstnesis, 83, 24.05.2007. https://likumi.lv/ta/id/157642

[22] European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[23] Saeima. Grozījumi Elektronisko sakaru likumā, 47th point. Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs, 2004, 23.nr. 2005, 12.nr, 2006, 24.nr. 47. Punkts. Available on: http://titania.saeima.lv/LIVS/SaeimaLIVS.nsf/0/1568E003526986C4C22572E300412301?OpenDocument Accessed April 4, 2020.

[24] Saeima. Grozījumi Elektronisko sakaru likumā. Latvijas Vēstnesis, 21, 30.01.2020. Available on: https://likumi.lv/ta/id/312285 . Accessed April 11, 2020.

[25] European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

is breaching fundamental human rights that are included in the Charter of fundamental rights of the European Union[26] or the European Convention on Human Rights[27].

Thirdly, during my research, the whole world faced COVID-19 pandemic and Latvian authorities used Electronic Communications Law as a tool to limit the spread of COVID-19.[28] In this part of the thesis I raised a question whether it is enough to declare national emergency for states to be excused of putting restrictions upon human rights. In order to raise a discussion I sent multiple questions to the Data State Inspectorate[29] and Ministry of Transport of the Republic of Latvia[30], because these are the institutions of competence over the Electronic Communications Law[31]. Once I received the answers, I argued whether I agree or disagree with them on the basis of my research results.

Fourthly, I explained that the right to privacy is more than we are used to believe. Privacy is a right of the individual that allows persons a free and uninterrupted participation in public affairs and the free use of other fundamental rights, thus privacy can be used as a condition for the sole existence of constitutional democracy.[32] Those rights can be restricted by states on multiple grounds, but the existing situation can be solved by other, less restrictive measures.

Lastly, this research shall aim at reaching a conclusion on the legality of the Electronic Communications Law. This aim will be reached by comparing the Directive 2006/24/EC[33] with the Electronic Communications Law and using both national and international case law in order to see how other states have dealt with this issue.

Research questions: Is national law breaching the right to private life and the right to the protection of personal data? Can this law, despite its validity be unjust? Are there any similarities

---

[26] The European Parliament. Charter of Fundamental Rights of the European Union, Article 7. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed March 15, 2020.

[27] The Council of Europe. European Convention on Human Rights, Article 8. Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf. Accessed March 4, 2020

[28] The State Chancellery. Stricter rules for physical distancing of persons are introduced to limit the spread of Covid-19. Available on: https://www.mk.gov.lv/en/aktualitates/stricter-rules-physical-distancing-persons-are-introduced-limit-spread-covid-19 Accessed April 4, 2020.

[29] Data State Inspectorate. Available on: https://www.dvi.gov.lv/en/ Accessed on April 14, 2020.

[30] The Ministry of Transport. Available on: http://www.sam.gov.lv/satmin/content/?cat=8 Accessed April 14, 2020.

[31] Saeima. Grozījumi Elektronisko sakaru likumā. Latvijas Vēstnesis, 21, 30.01.2020. Available on: https://likumi.lv/ta/id/312285 . Accessed April 11, 2020.

[32] Blanca R. Ruiz. Privacy in Telecommunications A European and an American Approach. Kluwer Law International the Hague, London, Boston. 1997 pp. 11-17.

[33] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

between the Electronic Communications Law and the Directive 2006/24/EC? If there is, would that be enough to declare national law invalid? Can Latvian authorities use the Electronic Communications Law to limit the spread of COVID-19, despite the fact that it could breach fundamental human rights?

1. The Directive 2006/24/EC

Firstly, in this thesis author will discuss the scope of the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (further - the Directive).[34] Secondly, author will move on to the Electronic Communications Law of Latvia and lastly, author will evaluate how and if the Directive has any similarities with the Electronic Communications Law of Latvia.[35]

The Directive[36] was adopted, because the existing electronic communications regulations could not regulate data retention as well as it was needed, thus the Directive amended the Directive 2002/58/EC.[37] After the Commission presented an impact assessment in relation to the rules on the retention of traffic data, the Directive was established on the basis of Article 95 of the Treaty establishing the European Community.[38]

On the 15 of March 2006 European Parliament and European Council passed the Directive.[39] According to Article 1, the aim of the Directive was to harmonise member states provisions concerning the obligations of the providers of publicly available electronic communications services and of public communications networks in order to ensure that the specific type of data can in the future be used for the purpose of the investigation, detection and prosecution of serious crime.[40]

---

[34] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[35] Elektronisko sakaru likums. Latvijas Vēstnesis, 183, 17.11.2004. Available on: https://likumi.lv/ta/id/9661 1 Accessed March 30, 2020.

[36] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[37] The European Parliament and of the European Council. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. Available on: http://data.europa.eu/eli/dir/2002/58/oj Acessed March 27, 2020.

[38] Kranenborg, Herke. "Protection of Personal Data." In The EU Charter of Fundamental Rights: A Commentary, edited by Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward, p. 223–224. London: Hart Publishing, 2014. Accessed June 5, 2020. Available on: http://dx.doi.org/10.5040/9781849468350.ch-009. Accessed April 4, 2020.

[39] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed Mach 21, 2020.

[40] The European Commission. Report from the Commission to the Council and the European Parliament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels. Available on: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF. Accessed April 7, 2020.; The

The Directive was not the first legal tool that regulated electronic communications. Before Directive, the European Union established two directives that dealt with data retention. First directive was Directive 95/46/EC that was established on the 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[41] This directive is no longer in force, because it was replaced by the Regulation 2016/679 mostly known as The General Data Protection Regulation on the 25 May 2018.[42] Second directive that was established by the European Parliament and the European Council was Directive 2002/58/EC[43] that was established on the 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.[44] This directive is still in force and can be seen as a successor of the Directive 95/46/EC.[45]

Almost twenty years ago, the Directive was a tool to combat terrorism, because terrorist attacks in Europe during 2004 and 2005 proved that Europe is not ready to combat such a high level of crimes.[46] The idea to trace terrorists using information from their phones and computers seemed like the best way how to make sure that terrorism attacks do not repeat itself.[47] Comparing the use of phones and computers then and now, it can be concluded that people's privacy was not violated as much as now. Back in the early 2000's social media were not a large part of people's life, not everybody used a computer or a mobile phone. Author agrees that the Directive, if it

---

European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 4, 2020.

[41]The European Parliament and European Council. Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available on: https://europa.eu/!Xb76Xu. Accessed April 7, 2020

[42] The European and European Council. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC Available on: http://data.europa.eu/eli/reg/2016/679/oj Accessed March 25, 2020.

[43] The European Parliament and the European Council. Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Available on: http://data.europa.eu/eli/dir/2002/58/oj Accessed March 26, 2020.

[44]Ibid..

[45] The European Parliament and of the European Council. The Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available on: https://europa.eu/!Xb76Xu. Accessed March 26, 2020.

[46] Richard A Posner, Not a Suicide Pact: The Constitution in a Time of National Emergency (Oxford, Oxford University Press, 2006).

[47] Møller Pedersen, Anja, Udsen, Henrik and Sandfeld Jakobsen, Søren (2018). "Data retention In Europe—the Tele 2 case and beyond". In: International Data Privacy Law p.160.; para 14(10) Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed March 27, 2020.

would not be invalidated, could be used as a tool to combat crime, but there is some level of doubt that two decades ago terrorists carried their phones around with them.

In the early years of the 21st century, the Directive was seen as a unique tool for law enforcement, because it was a new way how to combat crime in a newly established technology world.[48] According to Article 5 of the Directive[49], it authorised states to have an access to a wide variety of information to be obtained and stored by the telecommunication's providers. The Directive allowed to track almost all information regarding a call except the content of the call itself. Internet access providers also had the right to obtain a wide variety of information that established traffic data. All this information had to be stored and if needed, national and international authorities had the right to ask for this information. Since the information consisted of very personal information, the Directive did establish a level of protection for the obtained data. It was not easy to receive information about a person. In order to get access to the personal data for investigation purposes, police or other state security institutions had to ask a national court to grant them access to the needed information.[50] This information circulated not only between the authorities of the state, but also the Directive also allowed to exchange the stored information between all member states.[51]

Since terrorism and serious crime were a problem that one country could not battle alone, there was a need to create an identical way of gathering and storing data throughout the European Union.[52] Since all member states had different laws that consisted of different rules, it was up to

[48] The European Commission. Report from the Commission to the Council and the European Parlament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011 COM(2011) 225 final. Available on: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF Accessed March 25, 2020.

[49]The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[50] The European Union. Data protection and online privacy. Available on: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm Accessed April 2, 2020.

[51] Konstadinides, Theodore. "Mass Surveillance and Data Protection in EU Law – the Data Retention Directive Saga." In European Police and Criminal Law Co-operation, edited by Maria Bergström and Anna Jonsson Cornell, 69–84. London: Hart Publishing Ltd, 2014. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781474201568.ch-005. Accessed May 14, 2020.

[52] The Directive 2006/24/EC, Article 1. Available, last visited 27.03.2020; Konstadinides, Theodore. "Mass Surveillance and Data Protection in EU Law – the Data Retention Directive Saga." In *European Police and Criminal Law Co-operation*, edited by Maria Bergström and Anna Jonsson Cornell, 69–84. London: Hart Publishing Ltd, 2014. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781474201568.ch-005.

the Directive to harmonise data retention in the European Union.[53] The vision was that the providers of publicly available electronic communications services and public communications would ensure that the stored data is available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism.

Since the right to privacy existed long before any data protection regulation, upon the adoption of the Directive, the question of possible burdens to the fundamental right to privacy was raised.[54] During the adoption of the Directive, the European Parliament and the European Council concluded that the Directive was in compliance with the rights laid down in The Charter of Fundamental Rights of the European Union and with Article 7 and Article 8 of the European Convention of Human Rights, thus no possible violation of the right to privacy were found.[55]
After the Directive came into force, member states implemented it in their national laws of data retention or adopted a new law, using the Directive as a legal fundament. National laws and the Directive allowed legal national institutions to obtain information about person's habits, friends, and family.[56]

Legislators around Europe saw the Directive as a great tool to achieve greater security within the European Union. However, author sees this Directive as a mass surveillance tool.[57] This Directive violated fundamental rights in the name of security, there is no doubt that restrictions can be made, but restrictions that the Directive puts over the rights to privacy and personal data

[53] Brownsword, Roger, Eloise Scotford, Karen Yeung, Mark Leiser, and Andrew Murray. "The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies." In The Oxford Handbook of Law, Regulation and Technology.: Oxford University Press, 2017-07-20. Available: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199680832.001.0001/oxfordhb-9780199680832-e-2 Accessed April 7, 2020

[54] Konstadinides, Theodore. "Mass Surveillance and Data Protection in EU Law – the Data Retention Directive Saga." In European Police and Criminal Law Co-operation, edited by Maria Bergström and Anna Jonsson Cornell, 69–84. London: Hart Publishing Ltd, 2014. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781474201568.ch-005.

[55] Judgment of the Court (Grand Chamber), 8 April 2014. Joined Cases C‑293/12 and C‑594/12,para.24, Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed April 11, 2020.

[56] Stephen McGarvey, "The 2006 EC Data Retention Directive: A Systematic Failure," Hibernian Law Journal 10 (2011): 120. Available: https://heinonline.org/HOL/P?h=hein.journals/hiblj10&i=130 Accessed April 11, 2020.

[57] Konstadinides, Theodore. "Mass Surveillance and Data Protection in EU Law – the Data Retention Directive Saga." In European Police and Criminal Law Co-operation, edited by Maria Bergström and Anna Jonsson Cornell, 69–84. London: Hart Publishing Ltd, 2014. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781474201568.ch-005 .

are also violating the essence of the whole existence of the European Union. The values of the European Union are human dignity, freedom, democracy, equality, rule of law and human rights. Legal norms of the Directive breached all values of the European Union in the name of higher level of security within its borders and that is against the rules of democracy.[58]

Member states of the European Union have multiple law sources, for example countries constitution, legislation, and judicial decisions that can be developed into case law.[59] Despite the fact that member states have their own law and legal systems, none of the countries noticed any privacy infringements. The legal system, just as any other alive organism develops over time and grows. As the human rights grew, the Directive raised multiple questions about people's right to privacy, because people started to see that their human rights to privacy and privacy standards were violated.

1.1 Right to privacy and protection of personal data

The right to privacy is a right to control who and how information regarding the individual is used. This fundamental human right is set out in multiple[60] national and international human rights instruments. In this master thesis author will further focus on privacy that is regulated by the Charter of Fundamental Rights of the European Union[61] and the European Convention on Human Rights.[62]

Data protection and the right to privacy are inseparable rights.[63] However, they are not the same rights. Both rights are regulated by the Charter, but in theory they are two different freedoms.[64]

---

[58] European Union. The EU in brief. Available on: https://europa.eu/european-union/about-eu/eu-in-brief_en Accessed April 11, 2020.

[59] European E-Justice. Member States law. Available on: https://e-justice.europa.eu/content_member_state_law-6-en.do Accesswe April 11, 2020.

[60] United Nations. The Universal Declaration of Human Rights, Article 12. Available on: https://www.un.org/en/universal-declaration-human-rights/. Accessed April 11 2020.; The United Nations General Assembly. International Convenant on Civil and Political Rights, Article 17. Available on: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx Accessed April 12, 2020.; Latvijas Republikas Satversme. 96.pants. Latvijas Vēstnesis, 43, 01.07.1993. Available on: https://likumi.lv/ta/id/57980 Accessed April 12, 2020.

[61] The European Parliament, the Council and the Commission. Charter of Fundamental Rights of the European Union. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed April 10, 2020.

[62] The European Court of Human Rights. European Convention on Human Rights. Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf. Accessed on April 10, 2020.

[63] Patrik Hiselius, ICT/Internet and the Right to Privacy, Scandinavian Studies in Law 56 (2010), pp.201-208. Available on: https://scandinavianlaw.se/pdf/56-9.pdf Accessed April 12, 2020.

Yet, the legal issue that the Directive raised and that the Electronic Communication Law is raising, both freedoms cannot be separated.[65] In modern society, the right to privacy is a right to choose what information one keeps to himself and what information a person wants to share with the public. It is fair to say that the right to privacy is a right to be left alone, but in reality this right is a lot more complex than that.[66] Currently, international data protection rules are structured in a way that if ones data is collected, that person's privacy is safeguarded.[67] While the Directive was in force, the way how data was obtained and stored violated rights to privacy. In the second chapter of this thesis author will assess whether the same rights to private life and the right to data protection are breached by the Electronic Communications Law.

The right to privacy and protection of personal data are vital in assuring every individual's safety in the country they are living in. Governments are expected to protect individuals that are in their jurisdiction. That protection includes personal data protection.[68] However, the reality shows that governments use their powers and violate rights to privacy. Privacy is a right that goes hand in hand with human dignity which is an absolute human right.[69] Thus, privacy is not only an individual right but also a social value.

The surveillance effect that the lack of privacy can create is affecting multiple fundamental rights, either directly or indirectly. This effect was made by the Directive and could potentially be created by the Electronic Communications Law, through an interference with privacy and data protection rights affecting the enjoyment or exercise of other fundamental rights. Aside from privacy and data protection rights, surveillance can constitute an interference with such classic

---

[64] The European Parliament and the European Council. Charter of Fundamental Rights of the European Union. Privacy is regulated by the Article 8, but the right to protection of personal data is regulated in the Article 8 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT Accessed April 12, 2020.

[65] Corte, Lorenzo Dalla. A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection. In Data Protection and Privacy: Data Protection and Democracy, edited by Dara Hallinan, Ronald Leenes, Serge Gutwirth and Paul De Hert, 27–58. Computers, Privacy and Data Protection. Oxford: Hart Publishing, 2020.. Available on: http://dx.doi.org/10.5040/9781509932771.ch-002 . Accessed June 5, 2020.

[66] Patrik Hiselius, ICT/Internet and the Right to Privacy, Scandinavian Studies in Law 56 (2010): 201-208; Available on: https://ugp.rug.nl/GROJIL/article/view/31121/28428 Accessed April 11, 2020.

[67] The European Parliament. Personal data protection. Available on: https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection Accessed on April 12, 2020.

[68] Alexandra Rengel. Privacy as an International Human Right and the Right to Obscurity in Cyberspace. Groningen Journal of International Law, vol 2(2): Privacy in International Law, p. 38. Available on: https://www.researchgate.net/publication/328960219_Privacy_as_an_International_Human_Right_and_the_Right_to_Obscurity_in_Cyberspace Accessed April 11, 2020.

[69] The European Data Protection Supervisor. Data Protection. Available on: https://edps.europa.eu/data-protection/data-protection_en Accessed April 13, 2020.

civil and political rights as freedom of movement, freedom of association and assembly, freedom of expression and other rights.[70]

The digitalisation that has happened during the last 14 years shed a light to a need for higher level protection over personal life and data.[71] By strengthening the protection of personal data, the right to privacy is strengthened too. The same analogy applies, if one right is violated, then the other is also disturbed.

The right to privacy and data protection are important fundamental rights that are important for every person in the democratic society. Despite their importance, those rights as established by international public law are not an absolute human rights.[72] Both fundamental rights can be legitimately restricted by other overriding rights and they can also be illegitimately encroached upon, if the balancing test would conclude that the other conflicting right is more important. Greater cause usually is to safeguard other people's rights from terror or a crime, but such interfere can happen, if it is allowed by the law. If law allows to breach fundamental right, then the State must prove a legitimate aim. A legitimate aim is considered to be the protection of other people's rights, national security, public safety, prevention of crime and the protection of health.[73] When the legitimate aim is established, authorities of the state must prove that there is a necessity in the democratic society for such acts.[74]

---

[70] Ojanen, Tuomas. Rights-based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. In Surveillance, Privacy and Transatlantic Relations, edited by David D Cole, Federico Fabbrini and Stephen Schulhofer, 13–30. Hart Studies in Security and Justice. Oxford: Hart Publishing, 2017. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781509905447.ch-002.

[71] Corte, Lorenzo Dalla. A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection. In Data Protection and Privacy: Data Protection and Democracy, edited by Dara Hallinan, Ronald Leenes, Serge Gutwirth and Paul De Hert, 27–58. Computers, Privacy and Data Protection. Oxford: Hart Publishing, 2020. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781509932771.ch-002.

[72] Ojanen, Tuomas. Rights-based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. In Surveillance, Privacy and Transatlantic Relations, edited by David D Cole, Federico Fabbrini and Stephen Schulhofer, 13–30. Hart Studies in Security and Justice. Oxford: Hart Publishing, 2017. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781509905447.ch-002 Accessed on May 2, 2020.; Corte, Lorenzo Dalla. A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection. *In* Data Protection and Privacy: Data Protection and Democracy, edited by Dara Hallinan, Ronald Leenes, Serge Gutwirth and Paul De Hert, 27–58. Computers, Privacy and Data Protection. Oxford: Hart Publishing, 2020. Available on: http://dx.doi.org/10.5040/9781509932771.ch-002. Accessed June 5, 2020.

[73] Citizen advice. When can a public authority interfere with your human rights? Available on: https://www.citizensadvice.org.uk/law-and-courts/civil-rights/human-rights/when-can-a-public-authority-interfere-with-your-human-rights/ . Accessed March 8, 2020.

[74] Ibid.

Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[75], everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society.[76]

The Regulation (EU) 2016/679[77] (further - General Data Protection Regulation) lays down rules for the protection of individuals regarding the processing of personal data and rules relating to the free movement of personal data. Moreover, the General Data Protection Regulation protects fundamental rights and freedoms of all people, especially their right to the protection of personal data.[78]The General Data Protection Regulation is the newest tool that is adopted with the aim to protect fundamental human rights, more specifically, the right to privacy. It established a new way in safeguarding personal data in this social media century. The General Data Protection Regulation also pointed out that the data that indirectly points to a person is also considered to be personal data that must be safeguarded and thus, it falls under the scope of this law.[79]

Above mentioned proves that there is an active link between the legislation and the fundamental right to data protection.[80] Article 16 (1) of the Treaty on the Functioning of the European Union established that "*Everyone has the right to the protection of personal data concerning them.*"[81]

Article 4 of the Directive's preamble sets out restrictions that can be made, but only if all the conditions are met.[82] According to the preamble, restrictions can be made to safeguard national

[75] The European Court of Human Rights. European Convention on Human Rights. Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf Accessed on March 31, 2020.
[76] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 (08 April 2014, Para 14 (9) Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed April 12, 2020.
[77] The European Parliament and the Council of European Union. The Regulation (EU) 2016/679 of 27 April 2016 Official Journal of the European Union on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available on: http://data.europa.eu/eli/reg/2016/679/oj Accessed April 12, 2020.
[78]Ibid.
[79] The EU General Data Protection Regulation. Questions and answers. Available on: https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation Accessed May 17, 2020.
[80]Elise Muir. EU Equality Law. The First Fundamental Rights Policy of the EU, P.137. Oxford University press, Oxford, 2018.
[81]The European Union. Consolidated version of the Treaty on the Functioning of the European Union, Article 16 (1). Available on: http://data.europa.eu/eli/treaty/tfeu_2012/oj Accessed April 17, 2020.

security, defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.[83]

The restriction test is well-established and can be found in both national and international public law.[84] In order to restrict any right, states must prove that there is a necessity for the restrictions, that they are appropriate and proportionate in the democratic society and that they are made for specific public order purposes. Such purposes have to be valid, they cannot be made for unimportant reasons.[85]

It is important that the preamble sets out a norm that recognises fundamental rights and international public law principles that can be found in the Charter of Fundamental Rights of the European Union[86], because it reminds people that those are the basic rights that they have. Thus, creates a trust bond between an individual and the legislator. Further, the Directive clearly establishes that it is operating with respect and seeks to ensure full compliance with fundamental rights to respect for private life and communications and to the protection of personal data.

While the wording of the Directive sounded promising, the joined cases C‑293/12 and C‑594/12[87] showed that it takes much more than just a beautifully written preamble to prove and establish compliance with fundamental human rights.[88]

1.2 The Judgement of Digital Rights Ireland

---

[82] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[83] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[84] Peers, Steve, Tamara Hervey, Jeff Kenner, and Angela Ward, eds. The EU Charter of Fundamental Rights: A Commentary. London: Hart Publishing, 2014. Accessed June 12, 2020. http://dx.doi.org/10.5040/9781849468350.

[85] Article 29 Data Protection Working Party. Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005) p.4. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf Accessed May 12, 2020.

[86] The European Parliament, the Council and the Commission. Charter of fundamental rights of the European Union. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed May 12, 2020.

[87] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑594/12) EU:C:2014:238 (08 April 2014, Para 14 (9) Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed April 12, 2020.

[88] The Court of Justice of the European Union. The Court of Justice declares the Data Retention Directive to be invalid. Press Relase No 54/14 Luxembourg, 8 April 2014. Available on: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf Accessed on April 12,2020.

To compare the Directive and the Electronic Communications Law, it is important to look at the judgement that declares the Directive to be invalid. Further, this case is the most known case in the field of data retention even outside of the European Union, because the European Court of Justice tried to define the status of privacy and data protection rights in the legal system of the European Union, in the context of electronic surveillance, particularly the access to personal data.

In 2006 the Irish civil rights group "Digital Rights Ireland" brought a claim against the Irish Government in order to find out whether the Directive and the Irish national laws are fair in the light of the right to privacy.[89] The Digital Rights Ireland *TJ Mcintyre* publicly declared that " […] *laws require telephone companies and internet service providers to spy on all customers, logging their movements, their telephone calls, their emails, and their internet access, and to store that information for up to three years. This information can then be accessed without any court order or other adequate safeguard. We believe that this is a breach of fundamental rights.*"[90] Not only the Digital Rights of Ireland raised a question on the validity of the Directive[91], they also challenged the validity of national data retention law that was a part of the Irish Criminal Justice (Terrorist Offences) Act.[92]

Meanwhile, in Austria the same question was raised by the Government of the Province of Carinthia and by Mr Seitlinger, Mr Tschohl and 11128 people who were eager to find out whether the Directive and the national data retention law are compatible with the Federal Constitutional Law (Bundes-Verfassungsgesetz)[93], because applicants were convinced that both, the Directive and national data retention law are breaching fundamental human rights.

Only six years later, in 2012, the European Court of Justice received two requests for a preliminary ruling. One came from the High Court of Ireland and the other from the

[89] Digital Rights Ireland. DRI brings legal action over mass surveillance. Available on: https://www.digitalrights.ie/dri-brings-legal-action-over-mass-surveillance/ Accessed on May 10, 2020.
[90] Ibid.
[91] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY. Accessed on May 10, 2020.
[92] Irish Criminal Justice (Terrorist Offences) Act, 2005. Available on: http://www.irishstatutebook.ie/eli/2005/act/2/enacted/en/print.html Accessed on May 10, 2020.
[93] Austrian Federal Constitutional Law Bundes-Verfassungsgesetz. Available on: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1930_1/ERV_1930_1.pdf Accessed May 10, 2020.

Constitutional Court of Austria.[94] Despite the fact that cases came from two different countries, they both raised the same vital concern that the Directive violated fundamental human rights.[95]

The submitted questions by the parties could not be answered by the domestic courts, because national courts cannot evaluate whether the Directive is valid, therefor both questions were sent to the European Court of Justice. Since the addressed questions were identical in their essence, the European Court of Justice joined both cases together.

Firstly, to settle the case, the European Court of Justice examined how and whether two older directives, the Directive 95/46/EC[96] and the Directive 2002/58/EC safeguarded fundamental human rights to privacy. According to the findings[97], fundamental rights were safeguarded by the Directive 95/46/EC Article 1 (1)[98] and Article 17 (1)[99]. As for the Directive 2002/58/EC, the duty to safeguard fundamental rights was implemented in Article 1 (1)[100] and Article 4[101].[102] Thus, formally, the right to privacy was included in the Directive.

Both cases raised several different questions, but to combine cases, the European Court of Justice reduced all submitted questions to one general question. The overarching question was whether

---

[94] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 08 April 2014. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 . Accessed on May 9, 2020.

[95] Ibid.

[96] European Parliament and of the Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31). Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 Accessed on May 10, 2020.

[97] European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 (08 April 2014) Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed April 12, 2020.Accessed on May 9, 2020.

[98] The European Parliament and of the Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31). Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 Accessed on May 10, 2020.

[99] Ibid.

[100] The European Parliament and of the Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Article 1(1). Available on: http://data.europa.eu/eli/dir/2002/58/oj Accessed on May 12, 2020.

[101] Ibid.

[102] European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 (08 April 2014) Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020.

the Directive is valid in the light of Articles 7, 8 and 11 of the Charter of fundamental rights of the European Union.[103]

To answer the question, firstly, the court tackled whether freedom of expression is breached by the Directive. During this research author was surprised that the European Court of Justice even focused on this right, because in my opinion it is clear, that there is no link between the Directive and freedom of expression.

Freedom of expression is a right of each person to speak out opinions and share information in whatever form.[104] The right to expression also forbids governmental authorities or other individuals to practice censorship.[105] The core issue that the Directive upheld was not raising the issue of expression among people. The Directive allowed to store traffic and personal data such as caller ID and location, but such data have nothing to do with the right of expression. The European Court of Justice later in the case, found that the Directive has an effect on the fundamental right to respect for private life and the fundamental right to the protection of personal data that is regulated with the Articles 7 and 8 of the Charter of fundamental rights of the European Union. [106]

The European Court of Justice did not hesitate to point out that Article 3 and Article 5 of the Directive are problematic. If the information that is obtained according to the Directive, would be gathered about one individual, it would be possible to set out a map of everyday habits, home address, work address, it would provide information about individuals daily movements, the activities carried out, the social relationships of the individual and the social cycle that the person has.[107]

Author finds that this is a turning point of the whole case, because findings showed, that the data obtained go further and deeper into person's privacy than it is written in the Directive itself.

---

[103]The European Union. Charter of Fundamental Rights of the European Union. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed on April 16, 2020.
[104] Ibid. Article 11.
[105]Human rights guide. What is freedom of expression. Available onhttps://www.cilvektiesibugids.lv/en/themes/freedom-of-expression-media/freedom-of-expression/what-is-freedom-of-expression Accessed April 17, 2020.
[106] The European Union. Charter of Fundamental Rights of the European Union. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed on May 10, 2020.
[107] European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 (08 April 2014) Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020.

Subsequently, the wide roadmap of individual's private life, was declared to be a direct breach of Articles 7[108] and 8[109] of the Charter.[110]

The European Court of Justice used as important argument, that in order to prove that the breach of fundamental rights to privacy exist, it does not matter whether the information about the person concerned is sensitive or whether the person concerned have been inconvenienced in any way. [111] Further, the European Court of Justice used a case law[112] to prove that access of the competent national authorities to the data constitutes a breach of fundamental rights to privacy that are laid out in the Article 7 and Article 8[113] of the Charter. [114]

Advocate General *Cruz Villalon* in his opinion commented on Article 7 and Article 8 of the Charter.[115] The European Court of Justice[116] aligned with his comments and where that the fundamental rights are widely breached and that the breach can be qualified as serious.[117]

Suspicions of possible fundamental human rights violations existed, because the Directive allowed to obtain all kinds of data that was exposed to an unlimited number of persons for a long time. The Digital Ireland case developed and idea that the retention of data exclusively affects

---

[108] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 (08 April 2014) Para 36. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020.

[109] The European Union. Charter of Fundamental Rights of the European Union. Article 8. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed on May 10, 2020.

[110] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Para 29. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020.

[111] Ibid. Para 33..

[112] The European Court of Human Rights. Leander v. Sweden. Para. 48. Available on: http://hudoc.echr.coe.int/eng?i=001-57519 Accessed on May 10, 2020; European Court of Human Rights. Rotaru v. Romania no. 28341/95, para 46. Available on: http://www.hraction.org/wp-content/uploads/Rotaru_protiv_Rumunije.pdf Accessed on May 10, 2020; The European Court of Human Rights. Weber and Saravia v. Germany no. 54934/00, para 79. Available on: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-76586%22]} Accessed on May 10, 2020.

[113] European Union. The Charter of Fundamental Rights of the European Union. Article 7. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed on May 10, 2020.

[114] The European Parliament and European Council. Data Retention Directive 2006/24/EC Article 4 and Article 8 . Available on: http://data.europa.eu/eli/dir/2006/24/oj Accessed on May 10, 2020.

[115] Opinion of Mr Advocate General Cruz Villalón delivered on 12 December 2013. Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293 Accessed May 15, 2020.

[116] European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 (08 April 2014) para 37 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

[117] Ibid. Paras 77.-80.

those whose conduct in no way justifies the retention of data relating to them. The directive gives power to state actors to obtain almost unlimited information about people's private lives and use the obtained data for multiple purposes, having regard in particular to the unquantifiable number of persons having access to the data for a minimum period of six months, but up to two years. Because of the broad description in the Directive, it established legal doubts whether it can achieve the objectives which it pursues and if the proportionality of the interference with the fundamental rights is established.[118]

Before the European Court of Justice turned to the proportionality test, it stated that there is a ground to believe that the violation exists, because "[…] *data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter*."[119]

To conclude whether the Directive is lawful, the European Court of Justice applied a structured proportionality test that is set out in Article 4 of the Directive[120] and Article 52 of the Charter.[121] Even though the European Court of Justice and the Advocate General both concluded that the Directive is breaching the fundamental rights on a high level, it was not enough to announce the Directive invalid.

Next step was to test whether the breach of fundamental human rights could be justified or not. The first question of the test was whether the breach of fundamental rights satisfies an objective of general interest.[122]The court concluded that while the aim of the Directive was to harmonise

[118] European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 (08 April 2014) para 36 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[119]Ibid. Para 34.

[120] Ojanen, Tuomas. Rights-based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. In Surveillance, Privacy and Transatlantic Relations, edited by David D Cole, Federico Fabbrini and Stephen Schulhofer, 13–30. Hart Studies in Security and Justice. Oxford: Hart Publishing, 2017. 2020. Available on: http://dx.doi.org/10.5040/9781509905447.ch-002. Accessed May 12, 2020.

[121] European Union. The Charter of Fundamental Rights of the European Union. Article 7. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed on May 10, 2020.

[122] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Para 41. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

data retention in the European Union, the material objective according to Article 1 (1) was to contribute to the fight against serious crime and thus, ultimately, to public security.[123]

As mentioned before, state security is fundamental for everyone who is within the borders of a country. In the European Union, the neighbouring countries need to have sufficient security levels, so that everyone feels safe. The court also concluded that the fight against international terrorism in order to maintain international peace and security is considered to be a general interest of society.[124] During its evaluation, the court highlighted that the use of electronic communications are particularly important and can be a valuable tool in the prevention of offences and the fight against organised crime and crime per se.[125] Thus, despite all above mentioned fundamental rights violations, the Directive was seen as a great tool for crime combatting and subsequently it fully complies with the objective of general interest.[126]

Further, to make sure that the breach of fundamental rights is lawful, the European Court of Justice had to evaluate whether the interference was absolutely necessary in the democratic society.[127] Because the aim was fulfilled and the court saw the need to combat crime with new tools, it held that the retention of data for the purpose of allowing the competent national authorities to have possible access to personal data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.[128]

---

[123] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Para 41. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[124] Ibid. Para 36.

[125] Ibid. Para 43.

[126] Opinion of Mr Advocate General Cruz Villalón delivered on 12 December 2013. Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293 Accessed May 15, 2020. ; The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Para 42. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[127] Ojanen, Tuomas. Rights-based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. In Surveillance, Privacy and Transatlantic Relations, edited by David D Cole, Federico Fabbrini and Stephen Schulhofer, 13–30. Hart Studies in Security and Justice. Oxford: Hart Publishing, 2017. Available on: http://dx.doi.org/10.5040/9781509905447.ch-002. Accessed May 28, 2020.

[128] Citizens Advice. When can a public authority interfere with your human rights? Available on: https://www.citizensadvice.org.uk/law-and-courts/civil-rights/human-rights/when-can-a-public-authority-interfere-with-your-human-rights/, Accessed May 29, 2020; The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others,

Even though the European Court of Justice found the Directive to be a great tool for crime combatting, it turned to test the proportionality of the restrictions caused by the Directive. In order to evaluate the proportionality, the European Court of Justice had to weigh whether acts of the governmental authorities are appropriate for attaining the legitimate objectives pursued by the Directive and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.[129]

After close evaluation of the proportionality, the court concluded that crime combatting, especially fight against terrorism is indeed of the utmost importance in ensuring public security and its effectiveness may depend to a great extent on the use of modern investigation techniques.[130] However, such an objective of general interest, however fundamental it may be, does not justify a retention measure such as that established by the Directive being considered to be necessary for the purpose of combatting crime.[131]

Para 43 para 44. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[129] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 46. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020; The European Court of Justice. Case C‑343/09 Afton Chemical EU:C:2010:419, paragraph 45. Available on:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=ecli:ECLI:EU:C:2010:419 May 22, 2020; The European Court of Justice. Volker und Markus Schecke and Eifert EU:C:2010:662, paragraph 74. Available on: http://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=en Accessed May 30, 2020; The European Court of Justice. Cases C‑581/10 and C‑629/10 Nelson and Others EU:C:2012:657, paragraph 71. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0581 Accessed May 30, 2020.; The European Court of Justice. Case C‑283/11 Sky Österreich EU:C:2013:28, paragraph 50. Available on: http://curia.europa.eu/juris/document/document.jsf?text=&docid=132681&pageIndex=0&doclang=lv&mode=req&dir=&occ=first&part=1&cid=3638085 Accessed May 30, 2020; The European Court of Justice. Case C‑101/12 Schaible EU:C:2013:661, paragraph 29. Availabe on: http://curia.europa.eu/juris/document/document.jsf?text=&docid=143192&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3640430 Accessed May 30, 2020.

[130] Ojanen, Tuomas. Rights-based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. In Surveillance, Privacy and Transatlantic Relations, edited by David D Cole, Federico Fabbrini and Stephen Schulhofer, 13–30. Hart Studies in Security and Justice. Oxford: Hart Publishing, 2017. Available on: http://dx.doi.org/10.5040/9781509905447.ch-002 Accessed June 5, 2020.; The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 51. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020.

[131] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 51. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020.

The proportionality test proved that so far as it concerns the right to respect for private life, the protection of that fundamental right requires, according to the European Court of Justice settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.[132]

This judgement showed how the European Court of Justice chose to look between the lines of the Directive, because while author was reading the Directive, it never accrued how broad the scope of the Directive is. According to the courts findings, Article 3 of the Directive when read together with Article 5 (1) covers all types of electronic communications and covers all subscribers and registered users. Thus, it was concluded by the court that the Directive is interfering with the fundamental rights of practically the entire European Union's population.[133]

After the close examination, the European Court of Justice concluded that the scope of the Directive is too general, because according to the Directives rules, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.[134] The Directive affects all people who are using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies

[132] The European Court of Justice. Case C‑473/12 IPI EU:C:2013:715, paragraph 39. Available on: http://curia.europa.eu/juris/document/document.jsf?text=&docid=144217&pageIndex=0&doclang=lv&mode=req&dir=&occ=first&part=1&cid=3642011 Accessed June 1, 2020.; The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 52. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020.

[133] Ibid. Para 56.

[134] Konstadinides, Theodore. Mass Surveillance and Data Protection in EU Law – the Data Retention Directive Saga. In European Police and Criminal Law Co-operation, edited by Maria Bergström and Anna Jonsson Cornell, 69–84. London: Hart Publishing Ltd, 2014. Available on: http://dx.doi.org/10.5040/9781474201568.ch-005. Accessed June 5, 2020 ; The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 57. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.[135]

Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary. For the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.[136]

The lack of causal link between the data whose retention is provided for and a threat to public security, is not restricted to a retention in relation to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.[137]

The Directive practically, suspected each person of Europe to be a criminal, because according to the findings of the European Court of Justice, everyone who is using any type of device for communication could be a potential criminal. Further, the Directive does not require any link between the data whose retention is provided for and a threat to public security. [138]

The court discovered that another flaw of the Directive was that there were no limits to who can access to the data. The objective criteria by which to determine the limits of the access of the

[135] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 58. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020
[136] Ibid para. 62.
[137] Ibid. para 59.
[138] Ibid para 57.

competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concern offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, the Directive simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.[139]

The Directive does not mention any substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4[140] of the Directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.[141]

Further, the Directive[142] is lacking a norm that would specify how many people are authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures

[139] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 60. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[140] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[141] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 61. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[142] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.[143]

Another argument why the Directive lost its validity was due to the length of the period in which one was allowed to store data. Article 6 of the Directive[144] established a time limit from six months to a maximum of 24 months. Yet there was nothing written on when or what kind of data must be stored for period of time. The storage timeframe gave no objective criteria to ensure that it is limited to what is strictly necessary.[145]

The grave uncertainty of how to properly care for the obtained data was the last proof that was needed to declare that the Directive entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the European Union, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.[146]

All of the court findings proved that the protection of data retained by providers of publicly available electronic communications services or of public communications networks did not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. Moreover, Article 7 of the Directive had no rules which were specific and adapted to the vast quantity of data whose retention is required by that directive, the sensitive nature of that data and the risk of unlawful access to that data. These rules would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to

[143] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 62. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[144] The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[145] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 62-64. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ029 3 Accessed on May 9, 2020

[146] Ibid. paras 64.-65.

ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.[147]

The court found that the Directive did not set out limits for retained data sharing. While the Directive regulated data that had to be stored and obtained within the European Union, there were no restrictions for sending this data outside of the Europe. Because of that, the control, explicitly required by Article 8 (3) of the Charter[148], cannot be fulfilled by an independent authority of compliance with the requirements of protection and security. Sufficient control, carried out accordingly to the European Union law, is an essential component of the protection of individuals with regard to the processing of personal data.[149] Having regard to all the foregoing considerations, the European Court of Justice concluded that upon the adoption of the Directive, legislators have exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.[150]

The European Court of Justice declared that the Directive is lacking clear and precise rules that would govern the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Despite how great of a tool the Directive seemed to be, the interferences with fundamental rights were not justified.

The final judgement of the European Court of Justice[151] reminded Europe that fundamental human rights are the most important rights of all. It is important to note that while the judgement

---

[147] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 66. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[148] The European Parliament. Charter of Fundamental Rights of the European Union, Article 7. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed March 15, 2020.

[149] The European Court of Justice. Case C‑ 614/10 Commission v Austria EU:C:2012:631, paragraph 37. Available on:http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4660191 Accessed on April 17, 2020.; European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, para. 68. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on April 12, 2020. The European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[150] European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, para. 69. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 12, 2020.

[151] Court of Justice of the European Union Press Release No 54/14. Luxembourg, 8 April 2014. Available on: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf Accessed on April 16, 2020.;

was vital for this directive, it was not the first time that the arguments presented by the court came to light. Debates of whether the Directive is in line with the fundamental human rights started before the Directive was adopted.[152] In 2002 a Working Party that worked on previous data directives had sufficient doubts about the Directives legality due to the fact that it is so broad.[153]The Working Party claimed that terrorism was indeed a standing problem, but governments of the European Union should find a solution that does not ask to trade citizens' rights to live in peace and security in exchange for individual human right to data privacy, that is considered a cornerstone of modern democratic society.[154]

European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, para. 69. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 12, 2020.

[152] Ian Walden. Telecommunications Law and Regulation, Oxford University press, pp..599-603.

[153] Article 29 Data Protection Working Party. Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf Accessed on April 20, 2020.

[154] Ibid. p.2.

2. Electronic Communications Law

In the previous chapter author concluded that the Directive had two purposes. One was to harmonise data retention across the European Union and the other one was to combat crime in a modern way. In order to harmonise data retention, the Directive ordered member states to issue national law that obliged Internet access and telecommunications providers to obtain records of their user activity, as well as to keep all recorded data for up to two years, and provide access to stored data to the police and security services.[155]

Back on April 15, 2004 the Cabinet of Ministers issued the Electronic Communications Law according to the procedure of Article 81 of the Constitution on the 28th October of 2004, Saeima[156] adopted the Latvian Electronic Communications Law[157] that entered into force on the 1st of December 2004.[158] While the Electronic Communications Law was established prior to the Directive, legal norms included in this national law are arising from the Directive.[159] Articles were transposed from the Directive after it came in to force.

According to the *Saeimas* verbatim[160] report back in 2006 when the Directive came into force, the Electronic Communications Law was amended and during the amendment social impact assessment was applied to it. The test was used to see whether newly established norms have any impact on the society. The results of the impact assessment concluded that there was no impact on the society and that those norms could be transposed into the Electronic Communications Law.[161]

---

[155] Danny O'Brien. Data Retention Directive Invalid, says EU's Highest Court. April 8, 2014. Available on: https://www.eff.org/deeplinks/2014/04/data-retention-violates-human-rights-says-eus-highest-court. Accessed March 28, 2020.

[156] Ministru kabinets. Ministru kabineta noteikumi Nr.304. Available on: https://likumi.lv/ta/id/87151-elektronisko-sakaru-likums Accessed on March 28, 2020.

[157] 2020. gada 16. janvāra likums "Grozījumi Elektronisko sakaru likumā". Latvijas Vēstnesis, 21, 30.01.2020. https://likumi.lv/ta/id/312285 Accessed on March 28, 2020.

[158] Public Utilities Commission. Commissions Annual Report, p. 15. Available on: https://www.sprk.gov.lv/sites/default/files/editor/GadaParskati/SPRKgadaparskats2004.pdf Accessed March 28, 2020.

[159] European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[160] EU Open Data Portal. Verbatim reports of Saeima of the Republic of Latvia. Available on: https://data.europa.eu/euodp/en/data/dataset/elrc_1147 Accessed March 30, 2020.

[161] Grozījumi Elektronisko sakaru likumā, 47th point. Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs, 2004, 23.nr.; 2005, 12.nr., 2006, 24.nr. 47th point Available on:

The author would argue that the impact assessment was not applied in a proper way. The assessment only focused on the crime combatting, thus legislator tested the law only from one side. The Directive truly gave a unique tool for crime combatting, but that is not a justification for not evaluating the burden put upon the fundamental human rights. If the impact assessment would be applied correctly, then it would prove that existing legal norms are seriously affected, especially one fundamental human right.

The Electronic Communications Law consists of eight purposes. The first three purposes are regarding the electronic communications networks' development[162], next three purposes are about ensuring effective use of resources and protection of the State, providers, and users of electronic communications. The last three purposes are to protect personal data and ensure electronic communications services.[163] From all purposes, the purpose to ensure the protection of the interests of the State, users and electronic communications merchants[164] and the protection of user data, including personal data are in my view the most important ones.[165] They are the most important, because they are ensuring the right to privacy.

Despite the purposes of the Electronic Communications law, Annex 1 lays out several type of personal data that is allowed and must be retained by electronic communications services. They can obtain a telephone number that a person is calling to, the caller's name, surname, the name of the entity and its address. As well as the given name, surname or designation and address of the registered user called, and given name, surname or designation and address of the user to which the call is routed in the case of call forwarding.[166] That is already a huge amount of information, but it is also allowed to access data concerning how long person is speaking and data identifying the geographic location of each mobile communications network cell by reference to their location labels during the period for which communications data are retained.

Just like the Directive, internet access providers are also allowed to obtain a large amount of personal data. They have access to users name, surname, designation and address of the

---

http://titania.saeima.lv/LIVS/SaeimaLIVS.nsf/0/1568E003526986C4C22572E300412301?OpenDocument Accessed April 2, 2020.

[162] Latvijas Vēstnesis, Elektronisko sakaru likuma 2.pants. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed May 5, 2020.

[163] Ibid.

[164] Ibid. 2.panta sestais punkts.

[165] Ibid. 2.panta devītais punkts.

[166] Ibid. 1.pielikums.

subscriber or registered user to whom an Internet Protocol address, user ID or telephone number was allocated at the time of the connection.[167] If a person is using internet to call someone, the provider is allowed to obtain both phone numbers and information about both sides. Lastly, providers save information of time and date when a person logged in, logged off, sent an e-mail, or made a voice call.[168]

All the above mentioned personal data can be used for investigations lead by police, security agents or the Financial and Market Capital Commission (further - FKTK)[169]. FKTK is allowed to use data in order to perform the supervision specified in the laws and regulations in the field of protection of the collective interests of consumers and circulation of information society services, the Consumer Rights Protection Centre has the right to request.[170]

Further, personal data for example, of location can be obtained and transferred to pre-trial investigation institutions, bodies performing operational activities, state security institutions, the Prosecution Office and the court in order to protect the state and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings, as well as to the Competition Council for investigating violations of competition law which manifests as restrictive agreements. [171]

Information of person's name, surname, personal identity number or name, registration number, address, user ID, telephone number and location of such subscriber or registered user to whom Internet protocol address has been assigned during the connection has to be stored and transferred to the State Police to ensure the protection of the rights and legal interests of the persons offended in the electronic environment within cases regarding the physical and emotional abuse of a child.[172] All information can be obtained only if the court gives its permission.[173]

---

[167] Latvijas Vēstnesis, Elektronisko sakaru likums, otrais pielikums. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed May 5, 2020.
[168] Ibid. Otrais pielikums.
[169] The Financial and Market Capital Commission. Avaolable on: https://www.fktk.lv/en/ Accessed on June 4, 2020.
[170] Latvijas Vēstnesis, Elektronisko sakaru likums, 70.panta 8.1 punkts. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed May 5, 2020.
[171] Ibid. Otrais pielikums.
[172] Ibid. 71.pants.
[173] Ibid 2.pants.

Data that can be obtained by multiple state institutions for mostly investigation purposes is sensitive and if it would be leaked it would incredibly harmful to individuals and they would have a standing case to bring before the court for privacy infringements.

From what I have learned during my studies, I can see that from the perspective of European Union law and Public International law, the Electronic Communications Law is raising multiple privacy issues and could cause more if internet access provider servers would be hacked or if the electronic communications operators would face cyberattacks. Yet that is not enough to prove that the Electronic Communications Law is unlawful. In order to prove that this law is breaching a person's right to privacy an individual would have to go to court.

Currently, there is no national case, nor a study nor a publication that touches upon privacy issues that this law portraits. Does that mean that Latvian citizens have no problem with the fact that their rights to privacy are breached every day? Privacy is more than just a right to have a personal space at home. Privacy is a right of the individual that allows a person's free and uninterrupted participation in public affairs and the free use of other fundamental rights. Thus privacy can be used as a condition for the sole existence of a constitutional democracy.

Further in this chapter author will test whether the Latvian legislator is actively breaching rights to privacy of its citizens. Author raised this question, because the lack of awareness of this problem almost creates an illusion that the whole country somehow forgot about this law. Yet, that is not the case, because the law was amended in February 2020 and the use of it was widened in March 2020, but author will focus on the March amendments in the next chapter.

Since there are no publications regarding the fact that the Electronic Communications Law consists of norms that are directly taken from a Directive that seriously breached fundamental human rights, author is writing this master thesis in order to raise an awareness and to start a discussion among other professionals and the general public. It is important to raise awareness within the general public, because if the legislator will not announce the Electronic Communications Law unjust and invalid, there will be an urgent need to bring a case to the Constitutional court of Latvia, because it is the only court that can and arguably would announce that the existing law is not lawful.

In order to hear other opinions about the issue at hand, author have sent e-mails to the Data State Inspectorate[174] of Latvia and to the Ministry of Transport of the Republic of Latvia[175]. Author wanted to find out their view and their arguments on whether they find that the Electronic Communications Law is causing a burden on Latvian citizen's fundamental rights. To both institutions, author sent three questions. Firstly, whether it is allowed for telecommunications operators to give out retained data to medical personnel in order to combat the spread of COVID-19, knowing that the decision to give out private data is made without a consent of a judge? Secondly, author asked whether the research[176] by the University of Latvia and the SIA "*Latvijas Mobilais Telefons*" was concluded using the data that is specified in the Electronic Communications Law? If so, does the Data State Inspectorate see any violations of human rights, knowing that the Electronic Communications Law has no legal norm that would allow to use personal data for research purposes? Thirdly, author asked whether the Electronic Communications Law is violating Article 7 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention on Human Rights. While the questions author submitted were identical, the answers and the approach towards the questions were different.

The Data State Inspectorate (further – the Inspectorate) submitted the following answers[177]- firstly, the Inspectorate admitted that the data that consists of persons telephone number is a significant part of private life, thus giving this information out to any third party would constitute a breach of Latvian Constitution Article 96[178] and Article 8 of the European Convention on Human Rights.[179] Yet, as author expected prior to sending the question, the Inspectorate used the most universal argument - that the violation of human rights is justifiable if such acts are necessary for the achievement of a legitimate aim in a democratic society and is proportionate to its aim. In order to prove that their argument is valid, the Inspectorate used case law of the

[174] The Data State Inspectorate. Available on: https://www.dvi.gov.lv/en/ Accessed May 1, 2020.
[175] The Ministry of Transport of the Republic of Latvia. Available on: http://www.sam.gov.lv/satmin/content/?cat=134 Accessed on May 1, 2020.
[176] The annex of this thesis.
[177] The annex of this thesis.
[178] Latvijas Republikas Satversme, 96.pants. Latvijas Vēstnesis, 43, 01.07.1993. Available on: https://likumi.lv/ta/id/57980 Accessed on May 2, 2020.
[179] The European Court of Human Rights. European Convention on Human Rights. Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf Accessed May 2, 2020.

Constitutional Court of Latvia,[180] where the court has assessed whether a restriction of an individual's rights is justified.[181] The next argument presented by the Inspectorate was that according to the General Data Protection Regulation[182] if at least one point of the Article 6 (1) can be fulfilled, the use of data is lawful.

The answer and argument for the second question was divided in two parts. Firstly, the Inspectorate explained that according to the Article 71 of the Electronic Communications Law, emergency medical service has the right to have access to personal location data. Further, they listed all institutions that also have access to personal data. Secondly, they pointed out that according to Article 33 of the "On the Operation of State Authorities During the Emergency Situation Related to the Spread of COVID-19" [183] upon the request from the Centre for Disease Prevention and Control, the State Police has to provide the necessary personal information – location and the telephone number. Such information can be claimed only if the person is identified as a contact person for a person infected with Covid-19 or a person with a laboratory confirmed diagnosis of Covid-19. The State Police must transfer the data received from the electronic communications merchant to the Centre for Disease Prevention and Control for the performance of an epidemiological investigation. Thus, Data State Inspectorate concluded that the legal norm is not breaching fundamental human rights, because the grounds for the access to data can be found in Article 6 (1) (C) of the General Data Protection Regulation – *processing is necessary for compliance with a legal obligation to which the controller is subject* [184]

---

[180] Satversmes tiesa. 2003.gada 5.jūnija spriedums lietā Nr.2003-02-0106. Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2003-05-01_Spriedums.pdf Accessed on June 3, 2020.; Satversmes tiesa, 2003.gada 29.oktobra spriedums lietā Nr.2003-05-01. Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2003-05-01_Spriedums.pdf Accessed on June 3, 2020.; Satversmes tiesa. 1999.gada 6.jūlija sprieduma lietā Nr.04-02(99). Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/04-0299_Spriedums.pdf Accessed on June 3, 2020.

[181] Satversmes tiesa. 2010.gada 18.februāra spriedums lietā Nr.2009-74-01. Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2009-74-01_Spriedums.pdf Accessed on June 4, 2020.; Satversmes tiesa. 2011.gada 14.marta spriedums lietā Nr.2010-51-01. Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2015/06/2015-14-0103_Spriedums.pdf Accessed on June 4, 2020.

[182] European Parliament and the Council of the European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=LV Accesssed on May 27, 2020.

[183] Latvijas Vēstnesis. On the Operation of State Authorities During the Emergency Situation Related to the Spread of COVID-19. Available on: https://likumi.lv/ta/en/en/id/313730 Accessed on May 20, 2020

[184]European Parliament and the Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

Thirdly, to the last question, the Inspectorate argued that the research done by SIA "*Latvijas Mobilais Telefons*" and the University of Latvia does not show any sign of violation, but they also admitted that also have no information that actual personal data is used in this research. However, they turned to Article 71 of the Electronic Communications Law, that would allow such usage of data, if it would be done, because according to Article 71 (2)[185]: *the processing of location data for other purposes without the consent of a user or subscriber shall be permitted only in such cases if the user or subscriber cannot be identified using such location data*. Since the location data cannot be used to identify people, such usage is allowed.

The last question, whether the Electronic Communications Law is or is not violating fundamental human rights, was not answered, because the evaluation of validity is outside of its competence. Further, the Inspectorate stated that according to Article 16 of the Constitutional Court Law[186], the Constitutional Court hears cases regarding the compliance of other regulatory enactments or parts thereof, with legal norms (acts) of higher legal force. The same applies to the law "On the activities of state institutions during an emergency situation related to the spread of Covid-19".

The ministry of Transport used a different approach to the questions author submitted. They answered all three questions using the reference to the second question. Author was surprised that all those questions were approached the same way, considering that this answer was signed by the Secretary of State.

The answer to the first question was that according to Article 33 of on the Operation of State Authorities during the Emergency Situation Related to the Spread of COVID-19[187] law, the Centre for Disease Prevention and Control has a legal right to obtain location data and telephone number for epidemiological investigations. Unlike the Inspectorate who used Article 71[188] to prove that personal data is allowed to be used in case of investigation, the Ministry of Transport

---

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/oj

[185] Latvijas Vēstnesis. Elektronisko sakaru likums, 71.pants.183, 17.11.2004.Available on: https://likumi.lv/ta/id/96611 Accessed on May 17, 2020.

[186]Latvijas Vēstnesis. Satversmes tiesas likums. 103, 14.06.1996. https://likumi.lv/ta/id/63354 Accessed on May 20, 2020.

[187] Latvijas Vēstnesis. On the Operation of State Authorities During the Emergency Situation Related to the Spread of COVID-19. Available on: https://likumi.lv/ta/en/en/id/313730 Accessed on May 20, 2020

[188]Latvijas Vēstnesis, Elektronisko sakaru likums, 71.pants. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed April 7, 2020.

found the legal base for argument in the Regulation of the Cabinet of Ministers No. 820.[189] The essence of this argument is that the Centre for Disease Prevention and Control can obtain as much personal data as needed to fulfil its duties. Subsequently, since the legal norms allow to access such intervention, it is legal.

To the answer second question, the Ministry of Transport reached out to the University of Latvia and SIA "*Latvijas Mobilais Telefons*" and found out that the research was based on mobile network event statistics. Unfortunately, there is no such term in the Electronic Communications Law. The Ministry of Transport also used a term "general data". Author tried to find a meaning of above-mentioned terms in the Electronic Communications Law and found out that those terms do not exist.

Yet, the Ministry of Transport claimed that the level of data used in this research contains only general information that cannot identify the end user. Here, author would like to point out that the Directive also allowed to access general data, yet the European Court of Justice declared that the " general data" can pinpoint to a specific person, show people's habits and provide institutions with other data that, if put together can identify a person. The answer to the second question ended with a remark that the data used in this research is not regulated by the Electronic Communications Law, thus there is no violation towards use of personal data.

It is hard to believe that the last remark is true, because according to the information that is published by SIA "*Latvijas Mobilais Telefons*" , they used the location data that is regulated by the Electronic Communications Law. Otherwise, they could not reach two conclusions. Firstly, they concluded that because of the COVID-19 pandemic, people have returned to Latvia. Secondly, they wrote that "According to the data, the activity has moved from city and work centres to the residential area and rural area."[190] Further, they named multiple cities where higher

[189] Latvijas Vēstnesis, Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled. Available on: https://likumi.lv/ta/en/en/id/167539-procedures-by-which-pre-trial-investigative-institutions-bodies-performing-investigatory-operations-state-security-institutions-office-of-the-prosecutor-and-court-request-and-a-merchant-of-electronic-communications-transfers-data-to-be-retained-and-procedures-by-which-statistical-information-regarding-requests-of-data-to-be-retained-and-issuing-thereof-is-compiled Accessed on May 20, 2020.

[190] Latvijas Mobilais Telefons. LU un LMT pētījums: lielākoties iedzīvotāji ievēro norādījumu #paliecmājās. Available on: https://www.lmt.lv/lv/preses-relizes?pid=962 Accesed May 5, 2020. ; Latvijas Mobilais Telefons,

activity than usual has been detected. The fact that a research can detect movement proves that in this research location data has been used. Moreover, President of LMT prof. *Juris Binde* made a statement that "[…] *Secondly our data shows that all regions of Latvia comply with the requirement to stay home. At the same time, there are places where it is important to ensure that people do not violate the social distancing*." [191]

Lastly, this research concluded that according to the results ever since the state of emergency in the country was declared, both on weekdays and on weekends, the activity of people in certain places has rapidly increased - including in *Jūrmala* and *Salacgrīva*, where the number of visitors at other times of the year is quite small.

According to the information about the research author have concluded that there are two possible scenarios regarding the usage of data. Either this research is fake, or it is based on location data. To me it looks like they have used the location data, because at the end of the Press Release they have put a disclaimer that this research is conducted in accordance with the General Data Protection Regulation, but at the same time it allows to accurately assess the behaviour of the residents, as well as the location, movement and time of a particular activity.[192]

According to the General Data Protection Regulation[193], "[…] *processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's (...) behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her*."[194] Since the research used personal data

---

Latvijas Universitāte. Ārkārtas Pasākumu ievērošanas ietekme uz mobilko sakaru lietotāju uzvedību.Available on: http://lmt.mstatic.lv/lmt/files/2020/lu-lmt-petijums-/pezentacija.pdf Accessed June 11, 2020.

[191] LSM.lv ziņu redakcija. Mobilā tīkla pētījums: Lielākoties iedzīvotāji ievēro aicinājumu #paliecmājās. Available on: https://www.lsm.lv/raksts/dzive--stils/tehnologijas-un-zinatne/mobila-tikla-petijums-lielakoties-iedzivotaji-ievero-aicinajumu-paliecmajas.a354534/ Accessed April 7, 2020.

[192] Latvijas Mobilais Telefons. LU un LMT pētījums: lielākoties iedzīvotāji ievēro norādījumu #paliecmājās. Available on: https://www.lmt.lv/lv/preses-relizes?pid=962 Accesed May 5, 2020. ; Latvijas Mobilais Telefons, Latvijas Universitāte. Ārkārtas Pasākumu ievērošanas ietekme uz mobilko sakaru lietotāju uzvedību.Available on: http://lmt.mstatic.lv/lmt/files/2020/lu-lmt-petijums-/pezentacija.pdf Accessed June 11, 2020.

[193] The European Parliament and of the Council Regulation (EU) 2016/679 of the 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Preamble (71). Available on: https://eur-lex.europa.eu/eli/reg/2016/679/oj Accessed on March 28, 2020.

[194] The European Parliament and of the Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available on: https://eur-lex.europa.eu/legal-content/EN-LV/TXT/?uri=CELEX:32016R0679&from=EN Accessed April 5, 2020.

that included analysis of location and movements, this research is not held in accordance with the General Data Protection Regulation and it is breaching rights to privacy. Further, the usage of data is regulated with the Electronic Communications Law, even though the Ministry of Transport claimed otherwise.

The location data[195] is regulated by the Electronic Communications Law. Since the research used location information that is classifiable as personal data, with this research electronic communications merchant SIA "*Latvijas Mobilais Telefons*" has shared personal data with a third party – the University of Latvia. According to Article 71 (4) of the Electronic Communications Law, electronic communications merchant had to ask for persmission to ask if it could be transferred to third persons. In this case, SIA "*Latvijas Monilais Telefons*" illegally shared personal data for public research with a third party. Author find this to be a grave violation of personal data protection right. Thus, cannot agree with the ministry of Transport that this research is not violating human rights, because the usage of personal data for a public research that is conducted in collaboration with a third party without consent of the individual is highlighting that there are human right violations.

Since the Ministry of Transport focused only on the research, as soon as author received their answer, author sent another e-mail to them, to point out that they have not answered to the submitted *questions per se*.[196]The Ministry of Transport did not deliver the second answer within the legal time frame[197].

Both institutions claimed the same argument – violation of right to privacy is justifiable because such a violation is needed in order to maintain the highest possible level of state security, especially in times of a global pandemic. Author agrees with the fact that it is important, but the Electronic Communications Law is not the best tool to combat crime or a pandemic, since it is not even the aim of this law. Further, there is no link between a need to safeguard national security and the need to give out a broad spectrum of personal data to so many national and international institutions. The Directive prior to its invalidation provided national institutions with the same amount of information as the Electronic Communications Law. The European

[195] Latvijas Vēstnesis, Elektronisko sakaru likums, 1.panta piektā daļa, 1.un 2. pielikums. 183, 17.11.2004. Available on https://likumi.lv/ta/id/96611 Accessed April 5, 2020.
[196]On the May 29, 2020.
[197] Saeima. Iesniegumu likums, 5. Panta trešā daļa. Available on: https://m.likumi.lv/doc.php?id=164501 Accessed May 12, 2020.

Court of Justice claimed that this information, taken as a whole can provide authorities with a wide spectrum of personal information. The European Court of Justice concluded that the interference with private life of individuals cannot be justified. Since the Directive and the Electronic Communications Law are similar, therefor, the Electronic Communications Law is breaching fundamental rights.

Author believes that there is a standing case that needs to be brought to the court, because the Electronic Communications Law is directly breaching Article 8[198] of the European Convention on Human Rights that safeguards a person's right to private life.[199] In this chapter author will try to prove that the Electronic Communications Law is breaching human rights. Subsequently, if the breach will be proven successfully, author will test whether this breach is justifiable.

According to Public International Law and human rights, countries are allowed to interfere with human right due to public safety, national security and other crime related and important reasons.[200] In order to find out whether the plausible breach caused by national law is justifiable, it is necessary to test whether the breach satisfies the following criteria. In order to justify any limitations on human right, restrictions have to be in accordance with the law or prescribed by law and all restriction must be necessary in a democratic society.

To find out the necessity in a democratic society, author would have to turn to the European Court of Justice that often has to balance the people's interests that are protected by Article 8 and the member states' interests protected by other provisions of the convention and its protocols. In the next paragraphs author will analyse the plausible breach with the same test that the Latvian constitutional court would have to use if they were to deal with a case like this.

Firstly, the court would test, whether the law was adopted properly, in accordance with existing legal norms. The Electronic Communications Law was adopted in the correct time frame and

[198] The European Court of Human Rights. Guide on Article 8 of the Convention – Right to respect for private and family life. 2019, August 2019. Available: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf Accessed on March 28, 2020.
[199] Ibid. p.7.
[200] Huw Beverly-Smith, Ansgar Ohly, Agnes Lucas Schloetter. Privacy, Property and Personality Civil Law Perspectives on Commercial Appropriation., Cambridge Studies in intellectual property rights. P.218-219.; The European Court of Human Rights. Guide on Article 8 of the Convention – Right to respect for private and family life. P.7, August 2019. Available on: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf . Accessed on March 28, 2020.

was published in the official publisher of the Republic of Latvia, *Latvijas Vēstnesis*, thus there is no reason to doubt that the law was enacted with any procedural errors.[201]

Secondly, the Constitutional court would test whether the restrictions have a legitimate aim.[202] According to the Electronic Communications Law, all data, including traffic data that is obtained and stored by electronic communications providers and public internet service providers *per se* falls within the scope of Article 8.[203]

The reason why the state needs to have access to personal electronic data is to use it for case solving that involve organised crime groups, terrorism, and other state security related cases. According to the European Court of Justice, when a case is concerning terrorists, the States enjoy a wider margin of appreciation, especially with especially regarding the storage of information of individuals implicated in past terrorist activities.[204]

The European Court of Justice has found that it falls within the legitimate bounds of the process of investigation of terrorist crime for the competent authorities to record and retain basic personal details concerning the arrested person or even other persons present at the time and place of arrest.[205] In terrorism investigation cases it is proven that data retention is working, because a state can get a hold of person's data and use that collected data to safeguard society as a whole and maintain peace. There is no doubt that a breach of terrorist's or criminal's right to privacy is a smaller loss than a possibility to safeguard people's lives that would be harmed by the person who is being tracked by the state authorities.

Yet, the Electronic Communications law is not adopted for purely terrorism combatting purposes. This law allows to obtain data and use it for investigations, but it can also be used in a way that is without a necessity breaching people's right to privacy. For example, the law itself

---

[201] Latvijas Vēstnesis, Elektronisko sakaru likums, 71. pants. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 . Accessed April 7, 2020.

[202]Kaspars Balodis, Pamattiesību ierobežojuma konstitucionalitātes izvērtēšana Satversmes tiesas praksē. Rīgā, 2015.gada 11.decembrī.Available on: https://www.satv.tiesa.gov.lv/articles/pamattiesibu-ierobezojuma-konstitucionalitates-izvertesana-satversmes-tiesas-prakse/ Accessed April 10, 2020.

[203] The European Court of Human Rights. Guide on Article 8 of the Convention – Right to respect for private and family life. P.38, August 2019. Available: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf March 28, 2020.

[204] The European Court of Human Rights, judgment Segerstedt-Wiberg and Others v. Sweden 06.06.06 , para. 88. Available on : http://hudoc.echr.coe.int/eng?i=001-75591 Accessed March 29, 2020.

[205] Murray v. The United Kingdom, 18731/91, Council of Europe: European Commission on Human Rights, 27 August 1991, para 93. Available on: https://www.refworld.org/cases,COECOMMHR,402a22c44.html Accessed March 31, 2020.

allows to use data for solving cases of misdemeanours. There is no doubt, that this law helps to combat serious crimes and it is only a great tendency that police and other security agents are willing to use technology to combat crime. Author finds that existing consequences are too serious despite how great of a tool it is for the state. Thus, author would conclude that the legitimate aim exists, but the existing regulation is too broad, because obtained data can be used for all kinds of investigations.[206]

It is unacceptable to breach human rights for lower level crime investigations because human rights violations are proportionally causing more harm than misdemeanours. If the law would allow to use personal data strictly for terrorism combatting, then it would be appropriate, but while this is not the case, author finds this law to be too broad and therefor unlawful. Furthermore, while the legislator did not hesitate to set out nine purposes of the law, none of them mention that the aim is to combat crime.[207]

Thirdly, the court should conclude that, the Electronic Communications Law does not reach the necessity mark, since the human rights serve a greater importance in this particular situation.[208]Data retention is a modern tool, but this tool is used in a harmful matter. Currently, Latvia is using techniques that the European Court of Justice has found to be unacceptably weakening towards Article 8 of the Convention, because the existing regulation is allowing to obtain data without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.[209]

In a democratic society, the fact that the existing legislation that allows to screen its citizens in such a broad way using communications entails a threat of surveillance for all those to whom the legislation may be applied.[210]

---

[206] Latvijas Vēstnesis, Elektronisko sakaru likums, 71.pants. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 . Accessed April 7, 2020.
[207] Ibid. 2.pants.
[208] The European Union. Human Rights and democracy. Available on: https://europa.eu/european-union/topics/human-rights_en Accessed on April 7, 2020.; Latvijas Vēstnesis, Elektronisko sakaru likums, 71.pants. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 . Accessed April 7, 2020.
[209]European Court of Human Rights. Grand Chamber, Case of S. And Marper v. The United Kingdom, 4 December 2008, Para. 112. Available on: https://rm.coe.int/168067d216 Accessed April 7, 2020.
[210]The European Court of Human Rights, Weber and Saravia v. Germany, June 29, 2006, para. 78. Available on: http://hudoc.echr.coe.int/fre?i=001-76586 Accessed May 22, 2020.

Surely, there is an argument to be made that the domestic legislator and national authorities can, to a certain degree, assess what system of surveillance is required, but this power is not unlimited for countries with a democratic society. Powers of secret surveillance of citizens are tolerable only in so far as strictly necessary for safeguarding the democratic society.[211] Interferences that the Electronic Communications law allows must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued.[212]

If the law, as it in the case with the Electronic Communications Law, does not clearly indicate the scope and aim of the discretion conferred to the domestic authorities to obtain and store in a surveillance database information on person's private life, in particular, where it does not set out in a form accessible to the public any indication of the minimum safeguards against abuse, that amounts to an interference with private life as protected by Article 8 of the Convention.[213]

National law must provide sufficiently precise, effective and comprehensive safeguards on the ordering, execution and potential redressing of surveillance measures. Accordingly, the amount of privacy breach that the Electronic Communications Law is causing, could only be expectable if the need for the interference to be necessary in a democratic society would be interpreted as requirement that any restriction on person's rights are strictly necessary both, as a general consideration, to safeguard democratic institutions and, as a particular consideration, to obtain essential intelligence in an individual operation. If the restriction does not fulfil the criteria, state cannot issue any restrictions towards person's right to privacy.[214] To avoid stepping over an individual's right to privacy, data retention rules have to have clear and detailed rules, especially as the technology available for use is continually becoming more sophisticated.[215]

---

[211]European Court of Human Rights, Klass and Others v. Germany 6 September 1978, paras. 17.-42.Available on: http://hudoc.echr.coe.int/eng?i=001-57510. Accessed May 22, 2020.; Szabó and Vissy v. Hungary, no. 37138/14 12 January 2016, available: https://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf para 72-73

[212] European Court of Human Rights, judgment Segerstedt-Wiberg and Others v. Sweden 06.06.06, para 88. Available on: http://hudoc.echr.coe.int/eng?i=001-75591 Accessed May 22, 2020.

[213] European Court of Human Rights Shimovolos v. Russia, Application no. 30194/09, Council of Europe, 21 June 2011, available at: https://www.refworld.org/cases,ECHR,4e26e4d32.html Para 66,)

[214]Szabó and Vissy v. Hungary, no. 37138/14 12 January 2016, available: https://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf para 72-73

[215]European Court of Human Rights. Case of Kruslin v. France, Application no. 11801/85, para 33. Available on: http://hudoc.echr.coe.int/eng?i=001-57626. Accessed on May 12, 2020. ; European Court of Human Rights, Case of Huvig v. France (Application no. 11105/84) 24 April 1990. Available on: http://hudoc.echr.coe.int/eng?i=001-57627 Accessed on May 20, 2020.

No doubt that personal privacy is just as important as national security, because simultaneously national security is ensuring a person's security. It is important to point out that access to traffic data is useful and needed for combatting crime, however it is just as important to draw a line to how far countries can go when breaching privacy, keeping in mind that the rights that are at stake are fundamental rights to privacy.[216]

States are allowed to alter people's rights when balancing their interest in protecting national security through data retention measures against the seriousness of the interference with a person's right to respect for his or her private life. The national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, there must be adequate and effective safeguards against abuse of rights. In cases when the European Court of Justice has to weigh out states actions it has to take into account the circumstances of the case, such as the nature, scope and duration of measures.[217]

Article 8 of the European Convention of Human Rights is not the only international law article that the Electronic Communications is violating. Article 7 of the Charter of fundamental rights of the European Union[218] has also been breached. Exactly the same violation of Article 7 was found in the cases *Schrems*[219] *and Digital Rights*[220].

Author must admit, that despite the fact that Electronic Communications Law is violating human rights, the scheme that is used with this law is truly genius. Back in 2014 the Riga municipality proclaimed Riga to be the European Capital of Wi-Fi", because the municipality did a large project with the national telecommunications company "*Lattelecom*" that resulted in placing more than 4,000 free Wi-Fi points all around Riga.[221] In the past six years the count of public

---

[216] Stephen McGarvey, The 2006 EC Data Retention Directive: A Systematic Failure, Hibernian Law Journal 10 (2011)

[217] The European Court of Human Rights. Case of Roman Zakharov v. Russia, 4 December 2015, para 232 (Application no. 47143/06). Available on: http://hudoc.echr.coe.int/fre?i=001-159324 Accessed on May 20, 2020.

[218] The European Parliament, the Council, and the Commission. Charter of fundamental rights of the European Union. Article 7. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN Accessed on May 20, 2020.

[219] The European Court of Justice. Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 Accessed June 1, 2020.

[220] Judgment of the Court (Grand Chamber), 8 April 2014. Joined Cases C‑293/12 and C‑594/12,Para.24, Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed June 1, 2020.

[221] Latvian Public Broadcasting. Riga Names itself " European Capital of WiFi" July 3, 2014. Available on: https://eng.lsm.lv/article/economy/economy/riga-names-itself-european-capital-of-wifi.a90305/ Accessed June 2, 2020.

internet points has grown not only in Riga, but all across Latvia. People think that they are getting access to internet for free, but in reality, there are paying a very high price for it. People are giving away their identities and other vital information to the state authorities. This price way too high for a brief moment online.

There will be some, who will claim, that Google and other platforms like Twitter and Facebook are also doing the same thing and that is causing a bigger threat than what the national authorities do. It is important to point out that when human rights are at stake, there should not be a question of who is causing a bigger violation by their wrongful acts, because such acts are against people's rights to freedom, security and justice in the democratic country.[222]

Proof that governments are using data retention laws like the Electronic Communications Law can be found in the Google Transparency Record. Using this data base, everyone can find out how many times a government has filed a claim to gain access to personal data of its citizens.[223] The Government of Latvia have asked to have access to personal data of a few people and mostly received a decline. This fact also proves that Latvia mostly has no lawful reason to access data.[224]

2.1 New approach to the Electronic Communications Law

Another question that has to be considered is the aspect of national security and how broadly the Electronic Communications law can be used. On March 29, 2020 State Chancellery of Latvian Republic issued a statement that in order to control spread of the COVID-19 and for the purposes of conducting an epidemiological investigation and verifying the veracity of information on movement provided by a person and upon the request of the Centre for Disease Prevention and Control, the State Police will have the right to request information from electronic communications operators on specific persons who may have a status of the infected person or

[222] Payton, Theresa, Howard A. Schmidt, and Ted Claypoole. 2014. Privacy in the Age of Big Data : Recognizing Threats, Defending Your Rights, and Protecting Your Family. Lanham: Rowman & Littlefield Publishers. P. 33-44. Available on: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=688505&site=ehost-live. Accessed June 2, 2020.
[223] Google Transparency Report. Available on: https://transparencyreport.google.com/?hl=en Accessed June 2, 2020.
[224] Google Transparency Report on Latvia. Available on: https://transparencyreport.google.com/user-data/overview June 2, 2020.

contact person.[225] In my humble opinion there are other ways to tackle the problem and there is no need to widen the Electronic Communications law even more.[226]

As author have mentioned before, state security usually is the argument that countries are putting forward when they try to get excused for breaching human rights. As we all know by now, COVID-19 has caused a worldwide pandemic and countries are not only shutting down their boarders, but countries are also coming up with multiple new emergency laws in order to eliminate the spread of COVID-19. Latvia found a new way to make sure that COVID-19 is not spreading. The solution is simple, now there is no regulation on what grounds the Centre for Disease Prevention can ask for data. According to *Grozījumi Ministru kabineta 2020. gada 12. marta rīkojumā Nr. 103 "Par ārkārtējās situācijas izsludināšanu*" [227] they are allowed to ask for personal data if they have any suspicion that a person is breaching isolation rules or the person could harm others because he is ill with the virus. Rights to the medical personnel are given in order to safeguard national security and wellbeing. As mentioned before, in order to justify any compulsory and general data retention must be clearly demonstrated with evidence that is clear and raise no doubts.[228] The current situation allows to obtain data purely on doubts and fear and that is damaging the national legal system.

The existing legal framework without adequate safeguards of person's rights to privacy is also harming the European Union's legal framework.[229]The current national law is harmful, because freedom in all forms of communications is a dominant piece of modern society as a whole and

[225] State Chancellery. Stricter rules for physical distancing of persons are introduced to limit the spread of Covid-19. Available on: https://www.mk.gov.lv/en/aktualitates/stricter-rules-physical-distancing-persons-are-introduced-limit-spread-covid-19 last visited on 30.03.2020. Accessed June 2, 2020.; LETA. Mobilo sakaru operatori gatavi informēt par klientu aptuveno atrašanās vietu saistībā ar Covid-19. Available on: https://www.la.lv/mobilo-sakaru-operatori-gatavi-informet-par-klientu-aptuveno-atrasanas-vietu-saistiba-ar-covid-19 Accessed June 5, 2020.

[226]The European Court of Justice. Maximillian Schrems v Data Protection Commissioner, para. 94. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 Accessed June 5, 2020.

[227] Ministru kabineta 2020. gada 29. marta rīkojums Nr. 138 "Grozījumi Ministru kabineta 2020. gada 12. marta rīkojumā Nr. 103 "Par ārkārtējās situācijas izsludināšanu"". Latvijas Vēstnesis, 62D, 29.03.2020. Available on: https://likumi.lv/ta/id/313534 Accessed June 7, 2020.

[228] Article 29 Protection Working Party, 1868/05/EN WP 113, Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005) Adopted on 21st October 2005. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf Accessed April 1, 2020.

[229] Article 29 Protection Working Party, 1868/05/EN WP 113, Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005) Adopted on 21st October 2005, p.2. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf Accessed April 1, 2020.

the fundament of the European Union.[230] The right to privacy is set out in multiple European Union legislations and international law norms. It is included in all international human rights instruments and privacy has been recognised as an important right by courts all around the globe. It can be concluded that the right to privacy is part of customary international law.[231]

The European Court of Human Rights has pointed out that secret surveillance poses a danger to democratic society or it might destroy democracy and that States may not, as a tool against terrorism, adopt whatever measures they deem appropriate.[232] This statement can be applied in a situation of combatting a pandemic virus, because in both situations national security is at stake.

The Latvian legislator is treating obtained data as meaningless factual information, but in reality personal information that is allowed to obtain by law, is reflecting an identity of a person. This information is a key to get an exclusive glimpse of human life.[233]

The use of electronic communications data for combatting virus spread is unproportioned. Constitutional courts as well as the European Court of Human Rights and the European Court of Justice use the proportionality principle as a tool to safeguard fundamental human rights from acts by member states.[234] Proportionality principle requires for a state to put limitations on other rights according to the purpose and needs in the democratic society. It is a tool to weigh out the rationality of restrictions.[235]The proportionality is a complex principle, because it consists of adequacy, necessity and proportionality *stricto senus*.[236] In order to prove that the new state

---

[231] United Nations. The Universal Declaration of Human Rights. Availabnle on: https://www.un.org/en/universal-declaration-human-rights/ Accessed on June 3, 2020. ; United Nations Human Rights Office of the High Commissioner. The Right to Privacy in the Digital Age. Available on: https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx Accessed May 27, 2020. ; The European Parliament, the Council and the Commission. Charter of Fundamental Rights of the European Union. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed April 10, 2020.; The European Court of Human Rights. European Convention on Human Rights. Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf. Accessed on April 10, 2020.

[232]The European Court of Human Rights, Klass and Others v. Germany 6 September 1978, para. 49. Available on: http://hudoc.echr.coe.int/eng?i=001-57510 Accessed April 11, 2020.

[233] Marcin Betkier. Intersentia Studies on Law, Information and Technology. Privacy Online, Law and the Effective Regulation of Online Services, pp. 11-13. Intersentia, Cambridge, Antwerp, Chicago, 2019.

[234] Juan Cianciardo. Journal of Civil Law Studies, Volume 3 Number 1 Civil Law Workshop Saul Litvinoff Series, The Principle of Proportionality: The Challenges of Human Rights, 01.01.2020. Available on: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1028&context=jcls Accessed April 21, 2020.

[235] Juan Cianciardo Journal of Civil Law Studies, Volume 3 Number 1 Civil Law Workshop Saul Litvinoff Series, The Principle of Proportionality: The Challenges of Human Rights, 01.01.2020. Available: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1028&context=jcls Accessed April 21, 2020.178

[236] Ibid. p.179

emergency regulation towards the Electronic Communications Law is unproportioned, I will apply the proportionality principle.

First sub-principle is adequacy. It establishes that the law or a legal norm that is breaching human rights must achieve its purpose. Question here is whether it is possible to limit the spread of COVID-19 by tracking individuals' location. The first successful use of location data was reported on 10th of April, 2020.[237] According to the information published on the State Police website, a person who was COVID-19 positive left the house, despite the restrictions and obligation to self-quarantine. The person had to pay a fine of 2000 euro for breaching the law. It is the first reported case where the use of data was successful, so there is a proof that the use of the Electronic Communications Law can limit the movement of persons who are registered as virus positive. Yet, after paying the fine, it is likely that the individual will stay home. It is just as likely that this individual will leave his or her phone at home or will buy a pre-payed mobile card. In that way individual can no longer be tracked. I would argue that the aim can only be reached partially, thus new regulation is not adequate.

Second sub-principle is necessity which can be establish only, if the legislator has decided to use a restriction tool that is the least restrictive on human rights.[238] There are multiple privacy issues with the COVID-19 regulation, because it has many loop holes and uncertainties.

Latvia is not the first country who decided to track people by using their mobile or internet traffic data.[239] At first tracking started in Asia. The countries that suffered the most in Europe also took this idea and implemented it. Countries, including Latvia are using all means that they can come up with to fight this virus. There is a great need to combat COVID-19, but states have to remember no to step on fundamental rights unless it is the only means available to reach the aim.

---

[237] Valsts Policija, Vīrietim par stingras pašizolācijas neievērošanu piemēro maksimālo naudas sodu – 2000 eiro. Available: http://www.vp.gov.lv/?&relid=16869 last visited on 13.04.2020.

[238] Juan Cianciardo Journal of Civil Law Studies, Volume 3 Number 1 Civil Law Workshop Saul Litvinoff Series, The Principle of Proportionality: The Challenges of Human Rights, 01.01.2020. Juan Cianciardo. Available: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1028&context=jcls 179 Accessed April 21, 2020.

[239] Zack Doffman .COVID-19 Phone Location Trackin: Yes, It's Happening Now- Here's What You Should Know. Available on: https://www.forbes.com/sites/zakdoffman/2020/03/27/covid-19-phone-location-tracking-its-moving-fast-this-is-whats-happening-now/#48eff44611d3 Accessed March 27, 2020.

The Electronic Frontier Foundation[240] (further – the Frontier) has published its findings on the location surveillance. The Frontier strongly opposes individual location tracking.[241] According to their newest findings, countries that are tracking their citizens have not shown a significant success in combatting the spread of COVID-19.[242] Without actual proof that the use of data is the best tool in this global fight of COVID-19, there is no justification for breaching human rights. It is crucial to point out that the use of the Electronic Communications Law for virus combatting purposes is neither proportionate nor effective.

The Frontier highlighted another interesting aspect of the new regulations. Governments took this idea of location and data use from Asia, where Governments are usually not transparent about their actions towards their citizens. However, in Europe, Government transparency is vital. In the present case, not only Governments around the globe are not transparent, they are not transparent about their future plans regarding data tracking in the future.[243] In Latvia, there is no regulation on what is going to happen with obtained data in future, how long can data of COVID-19 positive persons be stored? COVID-19 is raising rage crimes against Chinese people. Wrongful storage of data that is obtained from people who suffer from COVID-19 could lead to a leakage of data and could potentially lead to multiple crimes that are driven by hate and fear of COVID-19.[244]

The location of the suspect in a COVID-19 case is breaching the principle of proportionality, because the same goal could be reached by a police officer. Instead of obtaining data of particular suspects who could be violating self-quarantine or isolation, the state police could make a randomised time home visit. If the person is not at home during the police visit, then

---

[240] The Electronic Frontier Foundation. About EFF. Available on: https://www.eff.org/about Accessed March 27, 2020.

[241] Supreme Court of the United Sates, Timothy Ivory Carpenter v. United Staes, No.16-402. Available on: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf . Accessed March 31, 2020.

[242] Zack Doffman. COVID-19 Phone Location Trackin: Yes, It's Happening Now- Here's What You Should Know. Available on: https://www.forbes.com/sites/zakdoffman/2020/03/27/covid-19-phone-location-tracking-its-moving-fast-this-is-whats-happening-now/#48eff44611d3 Accessed March 31, 2020.

[243] Ibid.

[244] Opinion by Emily Liu. Covid-19 has inflated racism against Asian-Americans. Here' s how to fights back., April 11, 2020. Available on: https://edition.cnn.com/2020/04/10/opinions/how-to-fight-bias-against-asian-americans-covid-19-liu/index.html Accessed March 31, 2020.; Evan Gerstmann, Irony: hate crimes surge against Asian Americans while they are on the front lines Fighting COVID-19. Available on: https://www.forbes.com/sites/evangerstmann/2020/04/04/irony-hate-crimes-surge-against-asian-americans-while-they-are-on-the-front-lines-fighting-covid-19/#40da15b53b70 Accessed March 31, 2020.; Carl Goldman, I recieved death threats for having coronavirus. 6 March 2020. Available on: https://www.bbc.com/news/av/world-us-canada-51761713/i-received-death-threats-for-having-coronavirus Accessed March 31, 2020.

person can be fined according to the law. I was one of those who returned to Latvia after boarders were already closed. During the quarantine I received multiple phone calls from the state police and the state police came once to check if I were truly at home. Since the new regulations allow to track only those who are COVID-19 positive I would propose two case scenarios that would be a lot more effective and also would also comply with human rights.

First way to limit the spread of the virus is similar to already existing regulations. As soon as a person is registered as a COVID-19 positive, a person should be asked to sign an agreement that their address of self-quarantine, name and surname can be used for national security reasons until the end of illness. Once the individual is home, in order to check whether person is home, the police should operate multiple home visits at different times of the day.

Second and more efficient way to combat COVID-19. When crossing a boarder and upon arrival in Latvia people should be required to fill out a form that consist of date of arrival, name, surname, address of a place where the person will isolate himself for the next 14 days. The State Police should gather this data with information from hospitals about persons who tested positive with COVID-19. All those who are in isolation should be checked regularly by home visits. This way the police would control those who are possibly ill because they were abroad. Since this virus was brought in by a traveller, it is not effective to only monitor those who are ill. Currently, for all travellers who just came back from their travels it is advised to stay at home, but there is no supervision. By monitoring all risk groups with the help of the police, the result of limitation would be reached better and in a less harmful way.

All the data that law enforcement currently has and that has been stored by internet providers gives a lot more information about the user. When a person is connected to a public internet provider, this provider is collecting that person's name, surname and location. It is then processing what each person is doing and with that it gains access to a person's interests, hobbies and even an occupation.[245]

[245] Zack Doffman. COVID-19 Phone Location Trackin: Yes, It's Happening Now- Here's What You Should Know. Available on: https://www.forbes.com/sites/zakdoffman/2020/03/27/covid-19-phone-location-tracking-its-moving-fast-this-is-whats-happening-now/#48eff44611d3 Accessed March 31, 2020.

Access to such data is granted with reasoning that in my opinion is way too broad. The legislator has to balance out a person's rights to privacy and interests of the state. With this particular law, author believes that Latvian authorities have more powers than it should have. [246]

In my opinion, all arguments mentioned above prove without a doubt that Latvia is breaching its obligations under the European Union law. The Current situation proves very strongly that there is an urgent need for a court judgement, because despite the already existing Electronic Communications Law that should not be in force, the Latvian legislator is widening its applicability range. It is proven over time by multiple countries that paper can take up all mistakes and the fact that a law is in force does not mean that the law is lawful.[247]

The existing legal problem is way too complex, and it is not solved by the existing framework. There is a need to set out more detailed provisions on how the obtained data can be used. Author would advise that particular situations are set out in which a state can ask for an individual's data. State security or national protection is too broad.

Recently, the situation in regarding to the national law became even more problematic, because due to the emergency situation national law is used to obtain data. The problem here is that emergency allows medical personnel to obtain information about a person solely because of the fear of the COVID-19. That is allowed, because data is obtained for national security reasons. At first, it seems to be valid, because Latvia is trying to limit the spread of COVID-19. However, there is no regulation mentioned in the law itself on how medical personnel must evaluate whether or not there is a need to obtain data. When it comes to providers, they have to blindly agree to give out personal data on the grounds of pure suspicion. National law is giving a medical professional a free card to obtain data, where, in my opinion, this should be evaluated by the first instance judge. New announcements also raise a question of how long medical personnel can keep this obtained data.

The use of private data should be the last resort, not just another tool to use in order to combat a virus. The general principles of international public law allows to obtain personal data only in

[246] Latvijas Vēstnesis. Elektronisko sakaru likums. 183, 17.11.2004. https://likumi.lv/ta/id/96611; Stephen McGarvey, The 2006 EC Data Retention Directive: A Systematic Failure, Hibernian Law Journal 10 (2011): 121

[247] Juan Cianciardo. Journal of Civil Law Studies, Volume 3 Number 1 Civil Law Workshop Saul Litvinoff Series, The Principle of Proportionality: The Challenges of Human Rights, 01.01.2020. Available on: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1028&context=jcls Accessed April 21, 2020.

order to achieve general interest, that in most cases means combatting truly serious crimes. The term serious crimes should also, for the sake of clarity be specified. Author would propose that the data of a private person should only be obtained in the situation of crimes against children, kidnapping, murder and terrorism. In the case *Digital Rights Ireland*[248] the European Court of Justice also criticised lack of clarity in what constitutes a "serious crime" and I agree with this court conclusion, because term "serious crime" is too broad.

In order for the law to pass the limitation test, it is needed to narrow down "serious crime". Only then limitations made to a person's right to privacy would be seen as appropriate, necessary and proportionate. Limitations cannot be put on persons who have done less serious crimes as it is in the case of limitations allowed in the COVID-19 context, because there simply are many other, less restrictive ways that can achieve the same aim, to limit the spread of the virus.[249]Police home visits are just as if not more effective than collecting data of a person's location. Existing electronic communications law is not proportionate for fighting the virus spread. Democratic values are breached by allowing the obtainment of data for this cause, because it is causing more risk to a person's privacy than it is doing good for the society as a whole. Thus, the new regulation is failing the test that is cumulative.

In the democratic country people trust state institutions to protect them and are no longer raising questions or testing the authorities whether they are truly acting on behalf of the democratic society and in their best interests.[250] The Electronic Communications Law allows to gather information of everyone, both innocent and guilty. There are also those, who willingly allow their data to be obtained by thinking that they have nothing to hide or there is nothing interesting happening in their lives. That is an alarming idea, because people are not aware or are in comfort

[248] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 08 April 2014. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 . Accessed on May 9, 2020.

[249]Article 29 Protection Working Party, 1868/05/EN WP 113, Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), p.6. Adopted on 21st October 2005. Available on : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pd Accessed June 1, 2020.

[250] Payton, Theresa, Howard A. Schmidt, and Ted Claypoole. 2014. Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. Lanham: Rowman & Littlefield Publishers. Pp. 33-36 Available on: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=688505&site=ehost-live. Accessed June 1, 2020.

that their human rights are being breached. No one can take away a person's human rights unless it is for a justifiable reason.

3. Correlation between Electronic Communications Law and the Directive 2006/24/EC

There are many similarities between the Directive[251] and the Electronic Communications Law. In this chapter author will analyse whether the Electronic Communications Law could be violating the same fundamental principles and have the same nature as the Directive. In previous chapters I explained why the Directive lost its force and what are the problematic aspect of the Electronic Communications Law before the emergency of a state was declared and what problems rose during the emergency situation caused by COVID - 19.

The European Court of Justice Judgement created a wave claims that were submitted to the national court all around Europe, because multiple national actors wanted to challenge their directive based national data retention laws. All claims were based on privacy infringement.

Sweden and the United Kingdom were the first countries to put their national data retention laws to the test, after the Directive became invalid. The European Court of Justice in a preliminary ruling held that national law[252] that allowed mass surveillance of electronic communications for the purpose of fighting crime, violated the right to privacy and the right to data protection.[253]In the joint case, an operator company from Sweden and a few private entities from the United Kingdom presented their national data retention laws just like in the Digital Rights Ireland[254] case of the Directive.

There is a direct link between Sweden's and the United Kingdom's data retention laws and the Latvian Electronic Communications law. Firstly, these laws consisted of norms that were taken directly from the Directive. Secondly, they all have a very broad regulation on when data have to be retained, who can ask for permission to access such data and they are lacking explanation on what is considered a state emergency. Thirdly, courts have found that existing regulations are placing unproportioned restrictions on the fundamental human rights. Thus, it can be concluded

[251] European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.
[252] Telecommunications Industry Dialog. Provision of real-time lawful interception assistance. Available on: http://www.telecomindustrydialogue.org/resources/sweden/ Accessed May 31, 2020.
[253] Joined Cases C-203/15 and C-698/15: Judgment of the Court (Grand Chamber) of 21 December 2016. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CA0203
[254] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 08 April 2014. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 . Accessed on May 9, 2020.

that there could be a standing case before the Constitutional court or the European Court of Justice against Latvia on the same grounds as in the Sweden and United Kingdom's joint cases.

There is an urgent need for at least an amendment of the Latvian national communications law. The Electronic Communications law, if not invalidated, then it should be amended in order to make sure it is in accordance with the Charter of Fundamental rights of the European Union and the European Union Convention of human rights so that a person's right to privacy is truly protected.

In the text of the law it is written that limitations are made only in the situation when there is a general interest of a state and public. While it is beautifully written and a general interest is the reason why and how states can interfere in people's rights, the existing law is way too broad to achieve the aim.

The effect of Covid-19 is not in line with the court finding in the Digital Rights Ireland.[255] The regulations violate the court's ruling, because the access of data of an individual is not reviewed by a court or independent administrative body. A review before access to data is important because the possibility of wrongful use is then lowered. There is also a need to have strict limitations on the retention period. The court did not take a final stance on existing national retention periods but indicates that a duration of six months has already been considered as reasonable. The European Court of Justice further requested that national laws expressly include an obligation to delete any retained data once its use is no longer necessary in combating serious crime. Currently, the Electronic Communications Law allows to store obtained data for more than six months and there are no norms that indicate how retained data should be stored or deleted. Moreover, because of the Covid-19 regulations, it even easier to access personal data, thus the violations of human rights are more visible and state actions are clearly harming human rights to privacy.

[255] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Cases C-293/12 and C‑ 594/12) EU:C:2014:238 08 April 2014. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 . Accessed on May 9, 2020.

In order to prove that the Latvian national position on data retention is against European Union's law, it is important to see how other member states of the European Union acted, after the Directive lost its validity.[256]

In June 2015, the Belgian Constitutional Court ruled that the national law implementing the Directive is no longer valid. Following the announcement, the Belgian legislator drafted a new law, based on the findings in the Digital Rights Ireland judgment. The new law fixed the flaws that the previous one had. Firstly, new amendments of a national law established proportionality because it allowed to obtain a person's data only in cases where it was a grave necessity.

Further, Belgium strictly narrowed down who can claim access to a person's data. Newly amended law introduced a norm that requires a crime to reach a certain level of seriousness in order to retain the data of a person. Lastly, the old time limit of how long data can be stored was shortened, allowing to store all data only for six months instead of one year. Interesting twist in the Belgium legislation was the fact that a few professions like lawyers and journalists were designated as a special protection group because of their profession aspects like right to not give up their source of information. The law was adopted on the May 29, 2016 and entered into effect on July 28, 2016.

France established its national data retention law back in June 21, 2004[257]. According to the law, electronic communications operators must retain specific data that could be necessary for investigations or the prosecution of criminal offence for the state authorities that are involved in this, as well as for other specific administrative or governmental authorities. French law allows to store data that consists of information that allows to identify phone user and the technical aspects of his or her communications. The French data retention law allows to store data for a period of one year.

The French law is almost identical to the Latvian Electronic Communications Law and they both came in force in the same year. Yet, there is one important difference. Unlike the Electronic Communications Law, the French supreme administrative court ruled that the French national law does not comply with the Charter of Fundamental Rights of the European Union because it is

[256] European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.
[257] Code of Posts and Electronic Communications ("CPEC") (Article L. 34-1) and its implementing regulations (Art. R. 10 12 and seq. CPEC

breaching fundamental rights to privacy. As mentioned before, the same argument towards privacy were made during the annulment of the Directive.

Germany also had its own national data retention law, that was established in accordance with the Directive.[258] In 2010 the German Constitutional Court declared that national data retention could no longer be in force. Later in 2015 the German legislator took the same steps as Belgium by establishing a new law[259] that consisted of more restrictions on who can ask for a person's data, as well as reduced the time limit of how long a provider store data up until ten weeks as well as divided the limit by establishing a lower time limit of only one month of location data. Unlike other countries I have researched, the Germany particularly focused on time limits. The Electronic Communications law has only very vague and broad time limits for data storage and there are no legal norms that would regulate when or how data must be erased. The German law also prohibits to store information about visited web pages and the location data can only be used in order to find the general geographic area of person. German data law also allows to store obtained data only in the cases of serious crimes, to obtain personal data in the cases of serious crime investigation and when there is a need to prevent a concrete danger to the state or to the life or liberty of a person.

Italy took a different approach than the other countries. The validity of the national data retention laws was challenged by Italian Data Protection Authority. The claim for a better regulation that is not violating human rights worked and the Italian Privacy Code was amended. New amendments changed how long providers can store personal data.

In March 2015, the Netherlands suspended the Dutch Telecommunications Data Act.[260] This decision was made in the light of Digital Rights Ireland judgment. However, the issue was raised

---

[258]German Archive. Telecommunications Act. Available on: https://germanlawarchive.iuscomp.org/?p=692&fbclid=IwAR2COL-ZNDtKc3_s-Lvnn4Q9RcAMNat_SD6UzvyQ083GfNMfAa1fHokHc6c Accessed June 4, 2020.; Darja Lončar Dušanovič, Implications of invalidity of Data Retention Directive to telecom operators. Available on: http://www.tribunajuridica.eu/arhiva/An4v2/5%20Darja.pdf?fbclid=IwAR2T9YSrE_ilEUI09ZwPvXhkWp764frqW3zb-UHlLe0xVMhxjFP4om0vNxE Accessed on Mar4ch 20, 2020.

[259] Paloma Bru; Laurent De Muyter; Jonathon Little; Mauricio F. Paez; Undine von Diemar The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws. Available on https://www.martindale.com/business-law/article_Jones-Day_2233580.htm Accessed on June 5, 2020.

[260] Library of Congress Law. Global Legal Monitor. Netherlands: Court Strikes Down Data Retention Law. Available on: https://www.loc.gov/law/foreign-news/article/netherlands-court-strikes-down-data-retention-law/ Accessed June 7, 2020.

not by a court or a national data agency. The validity question was raised by a member of the Dutch House of Representatives.[261] Furthermore, the Dutch Minister of Security and Justice has announced plans for a legislative proposal to amend the Telecommunications Act[262]and the Code of Criminal Procedure[263]in view of maintaining acceptable retention obligations under national law.

In Spain the Directive was implemented back in 2007, October 18 with national Law 25/2007.[264] The law allowed to obtain addresses and other data related to electronic communications and public communications networks. Unlike previously mentioned countries, the Spanish Constitutional Court found no violations of this law. However, the reasoning why the Spanish Constitutional Court found no issue with the law was simply because right after the Directive lost its validity, Spain amended its law by adding much stricter regulations, for example, that data can only be obtained if such information is needed for criminal investigations.

In the United Kingdom the Directive was implemented in 2009 with the Data Retention Regulations 2009. After the Directive was announced to be invalid, the United Kingdom passed the Data Retention and Investigatory Powers Act 2014. This act was established as a temporary tool to fill the holes that the Directive left. A year later, the United Kingdom's High Court held that the Act just like the Directive violated human rights.

Romania, just like other countries did their duty as a member of the European Union and adopted a national data retention law No. 298 and amended law No.506/2004.[265] Whenever the question of human right violations was raised, the government justified those possible violations with threats to national security. Despite government's arguments, in 2009 the Constitutional Court of Romania declared that both data retention laws are violating the rights of Romanian citizens to privacy and the court stated that there is a clear violations towards privacy and that laws cannot

---

[261] Tweede Kamer. Available on: https://www.houseofrepresentatives.nl/how-parliament-works/house-representatives-workAccessed June 7, 2020.

[262] Telecommunicatiewet. Available on: https://www.government.nl/documents/policy-notes/2012/06/07/dutch-telecommunications-act Accessed on March 31, 2020.

[263] Wetboek van Strafvordering

[264] The Libary of Congress. Online Privacy Law: Spain. Available on :https://www.loc.gov/law/help/online-privacy-law/2012/spain.php Accessed on June 2, 2020.

[265]The European Commission. Twelfth Annual Report of the Article 29 Working Party on Data Protection Available on: https://ec.europa.eu/justice/article-29/documentation/annual-report/files/2009/12th_annual_report_en.pdf Accessed on June 11, 2020.

meet with their purpose.[266] Unlike other countries, Romania proved that the Directive and laws that were established on grounds of it twice. Despite the arguments made by the Constitutional Court of Romania in 2009, the European Union forced to comply with the obligations and despite all arguments keep the national laws. As soon as the Directive lost its validity, the Constitutional Court, in 2014 declared that the national data retention laws are invalid, just like the Directive.[267]

In Austria, all data retention laws were declared invalid by the Constitutional Court in 27 June, 2014.[268] Decision was made due to the Ireland Digital Rights judgement of 8 March 2014.[269] Bulgarian Constitutional Court on 12 March 2015 found that national data retention laws are against Bulgarian constitution.[270]

There are some countries that currently have an active case before their Constitutional Courts. Those countries are the Czech Republic, Denmark, Hungary have found the relation with Tele2 judgement, but have still made no amendments to the law.[271] There are also countries like Croatia, Estonia, Finland, Poland[272] who have national data retention law that has not yet been challenged[273]

Overall, countries in the European Union have chosen to either establish a new data retention law or make amendments to the law that already exists. State practice shows that Latvia has two options. While the existing legal framework is causing harm to both the national and the

[266] Digital Rights Ireland, Romanian Constitutional Court holds data retention unconstitutional. Available on : https://www.digitalrights.ie/romanian-constitutional-court-holds-data-retention-unconstitutional/ Accessed May 20, 2020.
[267] IVPN. Privacy Laws in Romania. Available on: https://www.ivpn.net/internet-privacy-laws-in-romania#fn1 Accessed on May 20, 2020.
[268] The European Commission. Twelfth Annual Report of the Article 29 Working Party on Data Protection Available on: https://ec.europa.eu/justice/article-29/documentation/annual-report/files/2009/12th_annual_report_en.pdf Accessed on June 11, 2020.
[269] Ibid.
[270] Ibid.
[271] The European Commission. Twelfth Annual Report of the Article 29 Working Party on Data Protection Available on:\https://ec.europa.eu/justice/article-29/documentation/annual-report/files/2009/12th_annual_report_en.pdf Accessed on June 11, 2020.
[272] Telecommunications Act of 16 July 2004 (Consolidated text Journal of Laws of 12 October 2017 Available on: https://www.uke.gov.pl/en/law/ Accessed May 3, 2020.
[273] Council of the European Union. Working paper. Data retention – Situation in Member States. Available on: http://statewatch.org/news/2019/may/eu-council-data-retention-ms-situation-wk-3103-19.pdf Accessed May 20, 2020.

international legal system and to the human rights of Latvian citizens, the Electronic Communications Law could be amended in a way that would make it lawful and valid.

The law that regulates personal data must consist of incredibly clear measures and it must be used only in cases where there are threats of terrorism. Definitions should be set out clearly, without any space for wrongful interpretations.[274] The law needs to establish legal norms that sets out how to deal in a situation when fundamental human rights are infringed.

Technological evolution happens fast and sadly, as much as data privacy is evolving, has still not caught up to modern society needs and situations that seek regulation and because of that there is a strong need for regulation.[275] The Directive tried to seek harmonisation between member states but failed. The Electronic Communications law is currently used as a weapon to combat the spread of a pandemic virus, but it failed. What we are facing is an old problem in a new era, so the only path to safeguard fundamental rights is to end an era of laws that are generated from the Directive and establish new data retention laws that are applicable to this technology decade. Data that is obtained by technology made in 2020 cannot be regulated by a law that was established in 2004. It is time for technology related laws to grow.

The European Parliament in 2004 published a first report on the implementation of the Data Protection Directive 95/46/EC.[276] This report shows that the European Parliament was in fact truly concerned that the national data retention laws are not fully in accordance with rights that are granted by the European Convention of Human Rights, because they were described as unproportioned and unnecessary in the democratic society.[277] This is an argument that never

[274] Article 29 Protection Working Party, 1868/05/EN WP 113, Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005) Adopted on 21st October 2005. P.6 Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf Accessed April 1, 2020.
[275] Maricin Betkier. Privacy Online, Law and Effective Regulation of Online Services. P.41.-p.123.
[276] Report from the Commission. First Report on the implementation of the Data Protection Directive (95/46/EC). Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52003DC0265 Accessed on March 19, 2020.
[277] Council of Europe. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf Accessed on March 19, 2020.

reached the Latvian authorities, despite the fact that the Electronic Communications Law fully complies with the description made by the European Parliament.[278]

It is not possible to resolve issues that the Directive and the Electronic Communications Law have raised in the past and now. Yet, this master thesis is the first step towards informing the public of Latvia that our human rights have been breached for the last 14 years. In order to solve this issue, competent experts of data privacy, human rights experts and other experts have to come together.[279]

Just like the Directive, the Electronic Communications Law is causing legal uncertainty. Legal uncertainty exists because there are no strict provisions. The Electronic Communications Law is used to combat COVID-19, but is it clear from the legal norms, how and on what grounds medical personnel can ask for data? Will this data be used and how will it be deleted? All those questions remain unanswered.

The Directive never reached its goal and it is clear that neither will the Electronic Communications Law. The Latvian Centre for Disease Prevention and Control epidemiologist *Jurjis Perevoščikovs* gave a public statement that the use of the Electronic Communications Law is not useful for supervising whether a person is at home or not.[280] Further, the vice president *Ingmārs Pūķis* of Latvian Mobile Telephone spoke on the same issue. He claimed, that the location data is not as precise, thus it cannot be used for supervision purposes.[281]

---

[278]Darja Lončar Dušanovič, Implications of invalidity of Data Retention Directive to telecom operators p, 4-5.. Available on: http://www.tribunajuridica.eu/arhiva/An4v2/5%20Darja.pdf?fbclid=IwAR2T9YSrE_ilEUI09ZwPvXhkWp764frqW3zb-UHlLe0xVMhxjFP4om0vNxE Accessed on March 20, 2020.; Report from the Commission. First report on the implementation of the Data Protection Directive (95/46/EC). Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52003DC0265 Accessed on March 31, 2020.

[279]Darja Lončar Dušanovič, Implications of invalidity of Data Retention Directive to telecom operators. Available on :http://www.tribunajuridica.eu/arhiva/An4v2/5%20Darja.pdf?fbclid=IwAR2T9YSrE_ilEUI09ZwPvXhkWp764frqW3zb-UHlLe0xVMhxjFP4om0vNxE p.2, Accessed on June 1, 2020

[280]LTV " De Facto" Arī Latvijā top mobilo telefonu rīki Covid-19 kontrolei. Ko tas nozīmē privātumam? Available on:https://www.tvnet.lv/6953512/ari-latvija-top-mobilo-telefonu-riki-covid-19-kontrolei-ko-tas-nozime-privatumam?fbclid=IwAR15yF21ykzib-gVjIzx9-DYqEmmEkewGrE4T4hdQJ1zBCZ46xwOyeNY8sA Accessed on April 19, 2020.

[281] Ibid.

3.1 Arguments presented by the European Court of Justice

The similarities of the Directive and the Electronic Communications law uncourtly exist. To go even further, author decided to take the arguments used by the European Court of Justice and apply them to the Electronic Communications Law in order to see if they correspond.

The Electronic Communications Law and the Directive both allow to use obtained data for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism, in compliance with the rights laid down in Articles 7 and 8 of the Charter.[282] The European Court of Justice declared, that the obtained information can point to a specific person. The Directive did not have a complete list of information that it allowed to obtain, thus the court had to go through the whole Directive to find it out. Unlike the Directive, the Electronic Communications Law has Annex 1 and Annex 2 where all obtainable information is listed. Can the court's findings be applied in the case of the Electronic Communications Law? Yes, definitely, because it allows to obtain precisely the same information that the Directive allowed to obtained.[283] When Article 5 is placed next to both Annexes, it is clear that the Latvian legislator took Article 5 of the Directive, translated the text to Latvian, changed the order of words and directly copied it into the European Communications Law. Since the amount of information and type of data is identical, it can be concluded that the obtained data allows to precisely identify a person and its social circle. Information retained can show person's habits, places where person has lived, which routs a person takes and also identify relationships between people.

Bearing in mind that as of now, there is a regulation that allows to gain access to such information just on the ground of suspicion, the human rights violation could be gather that it was in the case of the Directive. The amount of information is also against the data protection

[282]The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.Para 24 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed May 28, 2020; Latvijas Vēstnesis, Elektronisko sakaru likuma 35.panta piektā daļa. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed May 5, 2020.

[283] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.Para 27 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed May 28, 2020.

requirements.[284] Further, author aligns with the Advocate General who pointed out[285] that the list of data that is allowed to be obtained is damaging the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector.[286]

The European Court of Justice has pointed out, that the fact that retained data can be reached by the competent national authorities also constitutes as an even further interference with the fundamental rights.[287] Because of the court's findings, it was concluded that the Directive's Article 4 and Article 8 violated the Article 7 of the Charter.[288] Access to the data according to the Electronic Communications law is granted to the Ministry of Transport[289]for the purpose of fulfilling the functions of the Ministry of Transport, State Joint-Stock Company Electronic Communications Office also has rights to receive the information necessary for the fulfilment of the functions of the State joint-stock company Electronic Communications Office.[290]

The Regulator can obtain information which is necessary for fulfilment of the functions of the Regulator.[291] The obtained data is available to the director of the Constitution Protection Bureau.[292] The Regulator after the receipt of a substantiated request, have ensure that the relevant information is accessible to the European Commission, the Latvian State administrative institutions and other European Union Member State regulators.[293] Further, all obtained data has

---

[284]The European Parliament and the Council. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available on: https://eur-lex.europa.eu/eli/reg/2016/679/oj Accessed May 16, 2020.

[285] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Paras. 39.-40. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[286] Ibid. Para 32.

[287] Ibid. para 35.

[288] The European Parliament. Charter of Fundamental Rights of the European Union, Article 7. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed March 15, 2020.; The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para. 35 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed May 9, 2020

[289] Latvijas Vēstnesis, Elektronisko sakaru likuma likuma 5 (4) pants. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed May 5, 2020. The Ministry of Transport. Available on: http://www.sam.gov.lv/satmin/content/?cat=8 Accessed April 14, 2020.

[290] Latvijas Vēstnesis, Elektronisko sakaru likuma 7.1.pants. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed May 5, 2020. State Joint-Stock Company Electronic Communications Office. Available on: https://www.vases.lv/en Accessed on May 6, 2020.

[291] Latvijas Vēstnesis, Elektronisko sakaru likuma 9. Panta pirmā daļa. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed May 5, 2020.

[292] Ibid. 19.panta pirmā daļa.

[293]Ibid. 35.panta piektā daļa. .

to be available to pre-trial investigation institutions, bodies .performing operational activities, the state security institutions, the Prosecution Office and the court in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings, as well as to the Competition Council for investigating violations of the competition law which manifests as restrictive agreements.[294]

All institutions that I have mentioned before show that the Electronic Communications Law gives access to obtained data to more institutions than the Directive. To my surprise, only Article 71[1] (1) mentions multiple institutions who can have access to the data.[295]This brings me to the conclusion, that the text hides the full list of institutions who can access the retention data. I had to look closely in order to find out who has access to the retained data. If a person would look over the law not so carefully, he would only see the institutions that are written in the Article 71.[1] (1).[296]

Another issue the author found with the articles that set out the institutions who can have access to the data is that they all are really broad. They all consist of a phrase: "[…] *is necessary for fulfilment of the functions*". [297] There is no description of what those functions are. Further, on the March 29, 2020 the Government of Latvia adopted stricter rules to limit the assembly of people at private and public events. Those restrictions included that for the purposes of conducting an epidemiological investigation and verifying the veracity of information on movement provided by a person and upon the request of the Centre for Disease Prevention and Control, the State Police will have the right to request information from electronic communications operators on specific persons who may have a status of infected person or contact person.[298]

The Latvian Minister of Health, *Ilze Vinķele* stated that stricter rules will not be used to find out what kind of routs people take. Rather, obtained data will be used only for epidemiological

[294] Latvijas Vēstnesis, Elektronisko sakaru likuma 71.[1] pirmā daļa. 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed May 5, 2020.
[295] Ibid.
[296] Ibid.
[297] Ibid.
[298] Cabinet of Ministers. Stricter rules for physical distancing of persons are introduced to limit the spread of Covid-19. Available on: https://www.mk.gov.lv/en/aktualitates/stricter-rules-physical-distancing-persons-are-introduced-limit-spread-covid-19 Accessed on May 14, 2020.

investigations.[299] The fact that the obtained data can be accessed by another institution and the fact that there are so many institutions that can use and claim data proves, that the Electronic Communications Law violates article 7 and Article 8 of the Charter[300]. A violation can be proved, because this law gives access to even more institutions than the Directive. Thus, the same argumentation that the European Court of Justice used can be applied to the situation at hand.[301]

Subsequently, the violation of fundamental human rights is serious and by widening the count of institutions who can have access to personal data, the government of Latvia could generate the feeling that private lives in Latvia are the subject of constant surveillance.[302]

As author have mentioned before, human rights can be restricted, but only if the limitation is necessary in a democratic society. In the case of the Directive, the European Court of Justice found that the Directive was used to combat terrorism and other serious crimes.[303] Subsequently, the Electronic Communications Law is also a tool to combat crime in Latvia. There is no need to use the Electronic Communications Law for terrorism combatting, because according to the information published by the Latvian State Security Service, the terrorism threat level in Latvia is low.[304]

---

[299] Tvnet. Sakaru operatoriem būs jāsniedz dati par Covid-19 inficēto vai to kontaktpersonu atrašanās vietu. Available on: https://www.tvnet.lv/6936296/sakaru-operatoriem-bus-jasniedz-dati-par-covid-19-inficeto-vai-to-kontaktpersonu-atrasanas-vietu Accessed on: May 14, 2020

[300] The European Parliament, the Council and the Commission. Charter of Fundamental Rights of the European Union. Available on: http://data.europa.eu/eli/treaty/char_2012/oj Accessed April 10, 2020

[301] Article 29 Protection Working Party, 1868/05/EN WP 113, Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005) Adopted on 21st October 2005. P.6 Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf Accessed April 1, 2020.
; The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para. 35 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[302] Ibid. Paras 37, 77.-80.

[303] Paloma Bru; Laurent De Muyter; Jonathon Little; Mauricio F. Paez; Undine von Diemar The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws. Available on https://www.martindale.com/business-law/article_Jones-Day_2233580.htm Accessed on June 5, 2020.; The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, para 37. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020.

[304] Latvian State Security Service. Latest news. Available on: https://www.vdd.gov.lv/en/ Accessed on May 15, 2020.

Despite the lack of terrorism, which is a great thing for Latvia, the Electronic Communications Law is, just like the Directive[305] ,a great tool for serious crime combatting and investigations. Crime combatting constitutes a state security matter, so there is no doubt, that some level of justification for human rights violations exists. But the level of justification is not so high that it would justify a retention measure such as that established by the Electronic Communications Law being necessary for the purpose of that fight.[306]

The Electronic Communications Law fails to lay down clear and precise rules on how data is stored, what the limits for accessing the data are and what constitutes a valid reason for obtaining personal data. The Directive failed to answer those questions and the European Court of Justice[307] pointed out that lack of answers to those questions are putting personal data at the risk of abuse, because no one can guarantee that the personal data will be used in accordance with law.[308] Same argumentation can be applied to the Electronic Communications law, because more state authorities have access to personal data and this law has no article that explains what should be understood by the phrase: "*necessary for fulfilment of the functions*". Thus, it can be concluded that the Electronic Communications Law, just like the Directive is putting retained personal data at the risk of unlawful use.[309]

The European Court of Justice concluded that the Directive was used in a way that went beyond what was strictly necessary, because it allowed to obtain personal data of the whole population of the European Union. Thus, the fundamental rights of all citizens of the European Union were

---

[305]The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para. 49 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[306] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para. 51 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[307] Paloma Bru; Laurent De Muyter; Jonathon Little; Mauricio F. Paez; Undine von Diemar The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws. Available on https://www.martindale.com/business-law/article_Jones-Day_2233580.htm Accessed on June 5, 2020. The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para. 54 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020.

[308] The Court of Human Rights, Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, paras. 62 and 63. Available on: https://hudoc.echr.coe.int/fre?i=001-87207 Accessed on June 1, 2020.

[309] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 54. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020; Paloma Bru; Laurent De Muyter; Jonathon Little; Mauricio F. Paez; Undine von Diemar The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws. Available on https://www.martindale.com/business-law/article_Jones-Day_2233580.htm Accessed on June 5, 2020

violated.[310] Surely, the Electronic Communications Law is not breaching human rights of the whole Europe. Yet, the personal data obtained by the Latvian institutions are allowed to be shared with all the European Union's member states, if it is necessary. How the Latvian institutions conclude what is necessary and what is not necessary is unknown. However, just like the Directive, the Electronic Communications Law covers, in a generalised manner, all Latvian citizens or residents that are in the jurisdiction of Latvia and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.[311] Is there really a link between a person and an unsolved crime? The answer is no, because even if there are no crimes and even if the person has not committed a single crime in his lifetime, his data will still be obtained and his data can be used as far as institutions find it necessary. How far is that? During my research the answer to this question was not found.

However, also those limits are causing an issue, because there is no separation on what kind of data is stored for a period that is lower than 18 or 24 months. Further, what happens to the data that cannot be longer stored? There is no regulation on how data must be erased. The fact that the Electronic Communication and the Directive are both limitless. The only limit that can be found in both legal instruments is how long data must be kept. For the Electronic Communications Law, the time limit is 18 months[312], but for the Directive it was a period not less than six months and not more than two years.

The Communications Law fails to set out clear and precise rules towards governing the extent of the interference with the fundamental rights that are granted to everyone by Articles 7 and 8 of the Charter. This proves that just like the Directive, the Electronic Communications Law entails a wide-ranging and particularly serious interference with those fundamental human rights.[313]

---

[310] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 56. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[311] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 57. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

[312] European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.

[313] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 65. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

Further, all the above mentioned issues with the Electronic Communications Law prove, that it fails to ensure rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks. Subsequently, national law cannot establish sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. Just like the Directive, the Electronic Communications Law does not lay down rules which are specific and adapted to the vast quantity of data whose retention is required by that directive, the sensitive nature of that data and the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. [314]

Author have applied the same arguments to the Electronic Communications Law, that the court used in the judgement that declared the Directive invalid. Last argument of the court was that the Directive did not comply with the principle of proportionality. Since all arguments presented by the court were applicable to the Electronic Communication Law, it can be concluded, that the law is also breaching the principle of proportionality.

Surely, author have no powers to declare a national law valid or invalid, but my research proves that the Electronic Communications Law is breaching the same fundamental human rights as the Directive was. The existing state of emergency in Latvia is causing an even deeper violation of fundamental rights, thus the arguments presented by the Ministry of Transport and the Data State Inspection are invalid and they cannot stand against the clearly visible arguments that origin from the comparison of the Directive and the Electronic Communications Law.

Lastly, there are no doubts that the right to privacy and data protection are not an absolute right. Such rights are balanced every day against other people's and state's needs. Personal data is used to combat crime and to safeguard people's health. Yet, in Latvia those restrictions upon the right to privacy and the right to personal data are unproportionate. As proven above, the Directive and the Electronic Communications Law are almost identical, thus the same violation of the right to privacy that the Directive put upon Europe, is currently visible in Latvia. The State institutions

[314] The European Court of Justice. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Para 66. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed on May 9, 2020

are using the same reservations as in the Digital rights Ireland case. They are hiding behind the state security argument, but none of the institutions have ever used the proportionality test to see, if Article 71 is truly applicable.

The European Court of Justice once already ruled that this kind of law instrument is invalid. The practice of multiple countries in the European Union has proved that the norms that were transposed from the Directive cannot be in force, because they are not just and are breaching human rights. stand with the honourable court, those member states who are pro data protection and pro privacy. The fact that the General Data Protection Regulation that safeguards human rights to privacy and data coexists with a disruptive Electronic Communications Law is simply not right.

During this research author also found out that the institutions in Latvia are following the written law. The received answers from the Ministry of Transport and the Data State Inspectorate both had the same argumentation – the Electronic Communications Law is valid, because the use of data in the name of state security is allowed. But if something is prescribed by law, is it always valid and just in the light of human rights? Author truly believes that anyone who will read this master thesis will conclude the same answer as author did. If not, there is a hope, that it will lead to a loud and successful discussion.

CONCLUSION

The main goal of the European Union is to ensure freedom, security and justice for all people who find themselves within its borders. To fulfil this goal, people have to trust in both, the European Union and their national legislator. Nevertheless, legislators have to keep the European Union's values in mind, when they are developing or adopting any regulations.[315]

There is no doubt that the most important rights are the fundamental human rights. The fundamental right to privacy ensures that the individual feel safe in the country they have chosen to live in. Fundamental human rights have to be protected in national and international level. To do so, there is a need to have a proper legal instrument.[316] The Directive was adopted with a good intentions, but as the European Court of Justice concluded, goal to ensure security cannot justify the violation of privacy. Author agrees with the European Court of Justice, that the retained data is a great tool to use during investigations, but the issue is how many and which state authorities can have access to personal data.

During this research, author have found multiple similarities that both the Directive and the Electronic Communications Law share. Both legal instruments are full of uncertainties and is lacking supervision aspect. According to the Electronic Communications Law, the access to personal data is not granted by a judge. Rather, this law consists of Articles that names those institutions who can have access to the data. The problematic aspect is all those norms consist of a phrase: "[…] *is necessary for fulfilment of the functions*". [317] Yet, there is no description of what those functions are or what is considered to be a necessity.

New regulations allow the Centre for Disease Prevention with the permission of the state police to gain access to personal data. Author concluded that such actions are against fundamental rights to privacy. Police upon the request from the Centre for Disease Prevention can share location data and phone numbers of a persons who are suffering from COVID-19 or there is a suspicion that a person could be ill. Just like the Directive, the new restrictions that are

[315] European Union. The EU in brief. Available on: https://europa.eu/european-union/about-eu/eu-in-brief_en Accessed June 11, 2020.
[316] United Nations. The Foundation of International Human Rights Law. Available on: https://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html Accessed June 11, 2020.
[317] Latvijas Vēstnesis. Elektronisko sakaru likums, 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed June 11, 2020.

established to ensure state security does not hold up to a proportionality principle, because there are more effective ways how to achieve the goal and not violate fundamental rights. Considering the powers of police, it would be better for a judge to declare whether it is truly necessary to gain access to data.

Even without the new regulations, the Electronic Communications Law is unjust and should be invalid. As the Ministry of Transport and the Data State Inspectorate pointed out, this law is used to combat serious crimes. Yet, as the author proved in this thesis, the use of this law for crime combatting is unproportioned. The same conclusion was made by the European Court of justice in regard to the Directive.

Further, in order to show the new habits of people in times of state emergency, the University of Latvia and the SIA "Latvijas Mobilais Telefons" conducted a research, that was concluded using the location data. According to the Constitution of Latvia[318] and the European Convention on Human Rights[319], sharing personal data with third parties is a violation of data protection.

All the above mentioned violations were found by the European Court of Justice. Those violations were the reason why the Directive became invalid. However, the Electronic Communications Law continues to cause widespread fundamental rights violations across Latvia and could cause more damage, if internet access provider servers would be hacked or if the electronic communications operators would face cyberattacks.

After comparing the Directive and the Electronic Communications Law, author concluded that the existing law have the same structure as the Directive. It almost looks like the Electronic Communications Law is a translated version of the Directive. Unfortunately, this law is also breaching the same fundamental rights. That is why it is important to follow the majority of member states, who invalidated their national retention laws, right after the Directive was declared to be invalid.

In the Republic of Latvia, were a sovereign and human rights are the top priority, there is no place for a law like this, which degrades the right to privacy. Author believes that this thesis is

[318] Latvijas Republikas Satversme, 96.pants. Latvijas Vēstnesis, 43, 01.07.1993. Available on: https://likumi.lv/ta/id/57980 Accesed June 10, 2020.
[319] The European Court of Human Rights. European Convention on Human Rights. Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf Accessed June 10, 2020.

the first step towards invalidation of the Electronic Communications Law, because it consists of arguments that needs to be presented to a wider public to show how their rights have been violated for the past 16 years.

BIBLIOGRAPHY

Primary sources

United Nations Documents

1. United Nations. The Universal Declaration of Human Rights. Available on: https://www.un.org/en/universal-declaration-human-rights/. Accessed on March 31, 2020.
2. The United Nations General Assembly. International Covenant on Civil and Political Rights. Available on: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. Accessed on March 31, 2020.
3. United Nations Human Rights Office of the High Commissioner. The Right to Privacy in the Digital Age. Available on: https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx. Accessed on March 31, 2020.
4. United Nations. The Foundation of International Human Rights Law. Available on: https://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html. Accessed on March 31, 2020.

International Legislation.

1. Council of Europe. European Convention on Human Rights. Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf. Accessed March 4, 2020.
2. European Parliament and European Council. Data Retention Directive 2006/24/EC. Available on: https://europa.eu/!dR36rY Accessed April 2, 2020.
3. European Parliament and European Council. Directive 2002/58/EC. Available on: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 Accessed April 9, 2020.
4. European Parliament and European Council. Directive 95/46/EC. Available on: https://europa.eu/!Xb76Xu . Accessed on April 14, 2020.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available on: http://data.europa.eu/eli/reg/2016/679/oj. Accessed June 1, 2020.

6. Directive 95/46/EC Available on: http://data.europa.eu/eli/reg/2016/679/oj Accessed June 1, 2020.
7. The European Parliament. Charter of Fundamental Rights of the European Union. Available on: http://data.europa.eu/eli/treaty/char_2012/oj.
8. The Treaty on the Functioning of the European Union Available on: http://data.europa.eu/eli/treaty/tfeu_2012/oj

Case Law

ECJ case law

1. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Available on: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN Accessed June 2, 2020.
2. Maximillian Schrems v Data Protection Commissioner, para. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 Accessed June 1, 2020.
3. Case C‑343/09 Afton Chemical EU:C:2010:419. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=ecli:ECLI:EU:C:2010:419 Accessed on May 22, 2020.
4. Volker und Markus Schecke and Eifert EU:C:2010:662. Available on: http://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=en Accessed May 30, 2020.
5. Cases C‑581/10 and C‑629/10 Nelson and Others EU:C:2012:657. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0581 Accessed May 30, 2020.
6. Case C‑283/11 Sky Österreich EU:C:2013:28. Available on: http://curia.europa.eu/juris/document/document.jsf;jsessionid=0E9EE95CB85951044AE02910FF8FA040?text=&docid=132681&pageIndex=0&doclang=LV&mode=lst&dir=&occ=first&part=1&cid=4719713 Accessed May 30, 2020.

7. The European Court of Justice. Case C‑ 101/12 Schaible EU:C:2013:661, paragraph 29. Availabe on: http://curia.europa.eu/juris/document/document.jsf?text=&docid=143192&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3640430 Accessed May 30, 2020.

ECHR case law

1. Weber and Saravia v. Germany, June 29, 2006. Available: http://hudoc.echr.coe.int/fre?i=001-76586 Accessed April 7, 2020

2. Szabó and Vissy v. Hungary, no. 37138/14 12 January 2016. Available on: https://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf Accessed April 10,2020.

3. Leander v. Sweden. no. 9248/81. Available on: http://hudoc.echr.coe.int/eng?i=001-57519 Accessed on May 10, 2020.

4. European Court of Human Rights. Rotaru v. Romania no. 28341/95, para 46. Available on: http://www.hraction.org/wp-content/uploads/Rotaru_protiv_Rumunije.pdf Accessed on May 10, 2020.

5. European Court of Human Rights. Weber and Saravia v. Germany no. 54934/00, para 79. Available on: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-76586%22]} Accessed on May 10, 2020.

6. Segerstedt-Wiberg and Others v. Sweden, no. 62332/00. Available on: http://hudoc.echr.coe.int/eng?i=001-75591 Accessed May 30, 2020.

7. Murray v. The United Kingdom, no. 18731/91, Council of Europe: European Commission on Human Rights, 27 August 1991, available on: https://www.refworld.org/cases,COECOMMHR,402a22c44.html . Accessed May 30, 2020.

8. Case of S. And Marper v. The United Kingdom, 30566/04, 4 December 2008, Available on: https://rm.coe.int/168067d216 . Accessed May 30, 2020.

9. European Court of Human Rights, Weber and Saravia v. Germany, no. 54934/00, June 29, 2006. Available: http://hudoc.echr.coe.int/fre?i=001-76586 Accessed May 30, 2020.

10. European Court of Human Rights, Klass and Others v. Germany 6 September 1978, http://hudoc.echr.coe.int/eng?i=001-57510. Accessed May 30, 2020.

11. European Court of Human Rights . Szabó and Vissy v. Hungary, no. 37138/14 12 January 2016, available: https://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf Accessed May 30, 2020.

12. European Court of Human Rights, judgment Segerstedt-Wiberg and Others v. Sweden 06.06.06 . Available: http://hudoc.echr.coe.int/eng?i=001-75591 Accessed May 30, 2020.

13. Shimovolos v. Russia, Application no. 30194/09, Council of Europe: European Court of Human Rights, 21 June 2011, available on: https://www.refworld.org/cases,ECHR,4e26e4d32.html Accessed May 30, 2020.

14. European Court of Human Rights, Case of Kruslin v. France, Application no. 11801/85, Available: http://hudoc.echr.coe.int/eng?i=001-57626 24 April 1990 para 33).

15. European Court of Human Rights, Case of Huvig v. France (Application no. 11105/84) 24 April 1990. Available: http://hudoc.echr.coe.int/eng?i=001-57627

16. European Court of Human Rights, Case of Roman Zakharov v. Russia 4 December 2015 (Application no. 47143/06), Available: http://hudoc.echr.coe.int/fre?i=001-159324. Accessed May 30, 2020.

17. The European Parliament and the Council. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available on: https://eur-lex.europa.eu/eli/reg/2016/679/oj Accessed May 16, 2020.

Constitutional Court of Latvia case law

1. Satversmes tiesa. 2003.gada 5.jūnija spriedums lietā Nr.2003-02-0106. Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2003-05-01_Spriedums.pdf Accessed on June 3, 2020.
2. Satversmes tiesa, 2003.gada 29.oktobra spriedums lietā Nr.2003-05-01. Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2003-05-01_Spriedums.pdf Accessed on June 3, 2020.

3. Satversmes tiesa. 1999.gada 6.jūlija sprieduma lietā Nr.04-02(99). Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/04-0299_Spriedums.pdf Accessed on June 3, 2020.
4. Satversmes tiesa. 2010.gada 18.februāra spriedums lietā Nr.2009-74-01. Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2009-74-01_Spriedums.pdf Accessed on June 4, 2020.
5. Satversmes tiesa. 2011.gada 14.marta spriedums lietā Nr.2010-51-01. Available on: http://www.satv.tiesa.gov.lv/wp-content/uploads/2015/06/2015-14-0103_Spriedums.pdf Accessed on June 4, 2020.

National legislation

1. Saeima. Grozījumi Elektronisko sakaru likumā. Latvijas Vēstnesis, 21, 30.01.2020. Available on: https://likumi.lv/ta/id/312285 . Accessed on April 11, 2020.
2. Grozījumi Elektronisko sakaru likumā, 47th point. Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs, 2004, 23.nr.; 2005, 12.nr., 2006, 24.nr. 47th point Available on:http://titania.saeima.lv/LIVS/SaeimaLIVS.nsf/0/1568E003526986C4C22572E300412301?OpenDocument. Accessed on June 2, 2020.
3. Irish Criminal Justice (Terrorist Offences) Act, 2005. Available on: http://www.irishstatutebook.ie/eli/2005/act/2/enacted/en/print.html Accessed on May 10, 2020.
4. Bundes-Verfassungsgesetz. Available on: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1930_1/ERV_1930_1.pdf Accessed on May 10, 2020.
5. Latvijas Vēstnesis. On the Operation of State Authorities During the Emergency Situation Related to the Spread of COVID-19. Available on: https://likumi.lv/ta/en/en/id/313730 Accessed on May 20, 2020.
6. Ministru kabineta 2020. gada 29. marta rīkojums Nr. 138 "Grozījumi Ministru kabineta 2020. gada 12. marta rīkojumā Nr. 103 "Par ārkārtējās situācijas izsludināšanu"". Latvijas Vēstnesis, 62D, 29.03.2020. Available on: https://likumi.lv/ta/id/313534 Accessed June 7, 2020.

7. Latvijas Vēstnesis. On the Operation of State Authorities During the Emergency Situation Related to the Spread of COVID-19. Available on: https://likumi.lv/ta/en/en/id/313730 Accessed on May 20, 2020.
8. Latvijas Vēstnesis, Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled. Available on: https://likumi.lv/ta/en/en/id/167539-procedures-by-which-pre-trial-investigative-institutions-bodies-performing-investigatory-operations-state-security-institutions-office-of-the-prosecutor-and-court-request-and-a-merchant-of-electronic-communications-transfers-data-to-be-retained-and-procedures-by-which-statistical-information-regarding-requests-of-data-to-be-retained-and-issuing-thereof-is-compiled Accessed on May 20, 2020.
9. Saeima. Iesniegumu likums, 5. Panta trešā daļa. Available on: https://m.likumi.lv/doc.php?id=164501 Accessed May 12, 2020State Chancellery. Stricter rules for physical distancing of persons are introduced to limit the spread of Covid-19. Available: https://www.mk.gov.lv/en/aktualitates/stricter-rules-physical-distancing-persons-are-introduced-limit-spread-covid-19 last visited on 30.03.2020. Accessed on May 20, 2020.
10. Ministru kabineta 2020. gada 29. marta rīkojums Nr. 138 "Grozījumi Ministru kabineta 2020. gada 12. marta rīkojumā Nr. 103 "Par ārkārtējās situācijas izsludināšanu"". Latvijas Vēstnesis, 62D, 29.03.2020.Available on: https://likumi.lv/ta/id/313534 Accessed on May 20, 2020.
11. German Archive. Telecommunications Act. Available on: https://germanlawarchive.iuscomp.org/?p=692&fbclid=IwAR2COL-ZNDtKc3_s-Lvnn4Q9RcAMNat_SD6UzvyQ083GfNMfAa1fHokHc6c. Accessed on May 20, 2020.
12. Telecommunications Act of 16 July 2004 (Consolidated text Journal of Laws of 12 October 2017 Available on: https://www.uke.gov.pl/en/law/ Accessed on May 20, 2020.
13. Telecommunications Act of 16 July 2004 (Consolidated text Journal of Laws of 12 October 2017 Available on: https://www.uke.gov.pl/en/law/ Accessed May 3, 2020.

14. Latvijas Vēstnesis. Elektronisko sakaru likums, 183, 17.11.2004. Available on: https://likumi.lv/ta/id/96611 Accessed March 30, 2020.

Other Official documents and papers

1. Article 29 Data Protection Working Party. Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005) Adopted on 21st October 2005. Available on https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf Accessed on May 22, 2020.
2. Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005) Adopted on 21st October 2005. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf Accessed on May 22, 2020.
3. Council of Europe. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 Available on: https://www.echr.coe.int/Documents/Convention_ENG.pdf Accessed on May 22, 2020.
4. Council of the European Union. Working paper. Data retention – Situation in Member States. Available on: http://statewatch.org/news/2019/may/eu-council-data-retention-ms-situation-wk-3103-19.pdf Accessed May 20, 2020.
5. Court of Justice of the European Union, The Court of Justice declares the Data Retention Directive to be invalid. Press Relase No 54/14 Luxembourg, 8 April 2014. Available on: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf Accessed on April 12, 2020.
6. European Commission, Report from the Commission to the Council and the European Parliament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011 COM (2011) 225. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF last visited on 25.03.2020. Accessed on May 22, 2020.

7. European Court of Human Rights. Guide on Article 8 of the Convention – Right to respect for private and family life. 2019, August 2019. Available: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf Accessed on May 22, 2020.
8. Privacy is regulated by the Article 8, but the right to protection of personal data is regulated in the Article 8 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT Accessed on May 22, 2020.
9. Report from the Commission to the Council and the European Parliament. Evaluation report on the Data Retention Directive. Available on: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A52011DC0225%3AEN%3AHTML Accessed on April 14, 2020.
10. Report from the Commission to the Council and the European Parliament. Evaluation report on the
11. The European Commission. Report from the Commission to the Council and the European Parliament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels. Available on: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF
12. The European Court of Human Rights. Guide on Article 8 of the Convention – Right to respect for private and family life. P.38, August 2019. Available: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf March 28, 2020.
13. Opinion of Mr Advocate General Cruz Villalón delivered on 12 December 2013. Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293 Accessed May 15, 2020.

Secondary sources

Books

1. Anabela Susana De Sousa Goncalves, "Extraterritorial Application of the EU Directive on Data Protection, The," Spanish Yearbook of International Law 19 (2015): 195-210 Available: https://heinonline.org/HOL/P?h=hein.intyb/spanyb0019&i=195 last visited on 02.04.2020.

2. Blanca R. Ruiz. Privacy in Telecommunications A European and an American Approach. Kluwer Law International The Hague, London, Boston. 1997 pp. 11-17.

3. Brownsword, Roger, Eloise Scotford, Karen Yeung, Mark Leiser, and Andrew Murray. The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies. In The Oxford Handbook of Law, Regulation and Technology. Oxford University Press, 2017-07-20. Available: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199680832.001.0001/oxfordhb-9780199680832-e-2 Accessed on May 23, 2020.

4. Corte, Lorenzo Dalla "A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection." In Data Protection and Privacy: Data Protection and Democracy, edited by Dara Hallinan, Ronald Leenes, Serge Gutwirth and Paul De Hert, 27–58. Computers, Privacy and Data Protection. Oxford: Hart Publishing, 2020. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781509932771.ch-002.

5. Elise Muir. EU Equality Law, the first fundamental rights policy of the EU. Oxford University press, Oxford, 2018 P.137

6. Huw Beverly-Smith, Ansgar Ohly, Agnes Lucas Schloetter. Privacy, Property and Personality Civil Law Perspectives on Commercial Appropriation., Cambridge Studies in intellectual property rights. P.218-219.

7. Intersentia Studies on Law, Information ans Technology. Privacy Online, Law and the Effective Regulation of Online Services, Marcin Betkier, Intersentia, Cambridge, Antwerp, Chicago, 2019.

8. Konstadinides, Theodore. "Mass Surveillance and Data Protection in EU Law – the Data Retention Directive Saga." In European Police and Criminal Law Co-operation, edited by Maria Bergström and Anna Jonsson Cornell, 69–84. London: Hart Publishing Ltd, 2014. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781474201568.ch-005 .

9. Kranenborg, Herke. "Protection of Personal Data." In The EU Charter of Fundamental Rights: A Commentary, edited by Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward, 223–266. London: Hart Publishing, 2014. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781849468350.ch-009. page 224

10. Kranenborg, Herke. "Protection of Personal Data." In The EU Charter of Fundamental Rights: A Commentary, edited by Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward, 223–266. London: Hart Publishing, 2014. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781849468350.ch-009. page 224
11. Marcin Betkier. Privacy Online, Law and the Effective Regulation of Online Services, pp. 79-100. Intersentia, Cambridge, Antwerp, Chicago, 2019.
12. Peers, Steve, Tamara Hervey, Jeff Kenner, and Angela Ward, eds. *The EU Charter of Fundamental Rights: A Commentary*. London: Hart Publishing, 2014. Accessed June 12, 2020. http://dx.doi.org/10.5040/9781849468350 .
13. Møller Pedersen, Anja, Udsen, Henrik and Sandfeld Jakobsen, Søren (2018). "Data retention In Europe—the Tele 2 case and beyond". In: International Data Privacy Law p.160.; para 14(10) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293
14. Ojanen, Tuomas. "Rights-based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union." In Surveillance, Privacy and Transatlantic Relations, edited by David D Cole, Federico Fabbrini and Stephen Schulhofer, 13–30. Hart Studies in Security and Justice. Oxford: Hart Publishing, 2017. Accessed June 5, 2020. http://dx.doi.org/10.5040/9781509905447.ch-002 .
15. Patrik Hiselius, "ICT/Internet and the Right to Privacy," Scandinavian Studies in Law 56 (2010): 201-208
16. Payton, Theresa, Howard A. Schmidt, and Ted Claypoole. 2014. Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. Lanham: Rowman & Littlefield Publishers. http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=688505&site=ehost-live. Accessed June 5, 2020.
17. Privacy, Property and Personality Civil Law Perspectives on Commercial Appropriation. Huw Beverly-Smith, Ansgar Ohly, Agnes Lucas Schloetter, Cambridge Studies in intellectual propperty rights.
18. Richard A Posner, Not a Suicide Pact: The Constitution in a Time of National Emergency (Oxford, Oxford University Press, 2006).

19. Stephen McGarvey, "The 2006 EC Data Retention Directive: A Systematic Failure," Hibernian Law Journal 10 (2011): 120. Available: https://heinonline.org/HOL/P?h=hein.journals/hiblj10&i=130

20. Telecommunications Law and Regulation, Oxford University press, Ian Walden. P.599-603.

Web sources

1. Cabinet of Ministers. Stricter rules for physical distancing of persons are introduced to limit the spread of Covid-19. Available on: https://www.mk.gov.lv/en/aktualitates/stricter-rules-physical-distancing-persons-are-introduced-limit-spread-covid-19 Accessed June 11, 2020
2. Carl Goldman, I recieved death threats for having coronavirus.Available on: https://www.bbc.com/news/av/world-us-canada-51761713/i-received-death-threats-for-having-coronavirus. Accessed June 11, 2020
3. Darja Lončar Dušanovič, Implications of invalidity of Data Retention Directive to telecom operators. Available on: http://www.tribunajuridica.eu/arhiva/An4v2/5%20Darja.pdf?fbclid=IwAR2T9YSrE_ilEUI09ZwPvXhkWp764frqW3zb-UHlLe0xVMhxjFP4om0vNxE Accessed June 11, 2020.
4. Data State Inspectorate. Available on: https://www.dvi.gov.lv/en/ Accessed June 11, 2020
5. Digital Rights Ireland, Romanian Constitutional Court holds data retention unconstitutional. Available on : https://www.digitalrights.ie/romanian-constitutional-court-holds-data-retention-unconstitutional/ Accessed May 20, 2020.
6. European Union. The EU in brief. Available on: https://europa.eu/european-union/about-eu/eu-in-brief_en Accessed June 11, 2020.
7. Evan Gerstmann, Irony: hate crimes surge against Asian Americans while they are on the front lines Fighting COVID-19. Available on: https://www.forbes.com/sites/evangerstmann/2020/04/04/irony-hate-crimes-surge-against-asian-americans-while-they-are-on-the-front-lines-fighting-covid-19/#40da15b53b70 Accessed June 11, 2020.
8. Google Transparency Report on Latvia. Available on: https://transparencyreport.google.com/user-data/overview Accessed June 11, 2020

9. Google Transparency Report. Available on: https://transparencyreport.google.com/?hl=en Accessed June 2, 2020.
10. IVPN. Privacy Laws in Romania. Available on: https://www.ivpn.net/internet-privacy-laws-in-romania#fn1 Accessed on May 20, 2020.
11. Journal of Civil Law Studies, Volume 3 Number 1 Civil Law Workshop Saul Litvinoff Series, The Principle of Proportionality: The Challenges of Human Rights, 01.01.2020. Juan Cianciardo. Available: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1028&context=jcls Accessed June 11, 2020.
12. Juan Cianciardo. Journal of Civil Law Studies, Volume 3 Number 1 Civil Law Workshop Saul Litvinoff Series, The Principle of Proportionality: The Challenges of Human Rights, 01.01.2020. Available on: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1028&context=jcls . Accessed June 11, 2020.
13. Kaspars Balodis, Pamattiesību ierobežojuma konstitucionalitātes izvērtēšana Satversmes tiesas praksē. Rīgā, 2015.gada 11.decembrī.Available on: https://www.satv.tiesa.gov.lv/articles/pamattiesibu-ierobezojuma-konstitucionalitates-izvertesana-satversmes-tiesas-prakse/ Accessed April 10, 2020.
14. Kranenborg, Herke. "Protection of Personal Data." In The EU Charter of Fundamental Rights: A Commentary, edited by Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward, p. 223–224. London: Hart Publishing, 2014. Accessed June 5, 2020. Available on: http://dx.doi.org/10.5040/9781849468350.ch-009. Accessed April 4, 2020.
15. Latvian Public Broadcasting. Riga Names itself " European Capital of WiFi" July 3, 2014. Available on: https://eng.lsm.lv/article/economy/economy/riga-names-itself-european-capital-of-wifi.a90305/ Accessed June 2, 2020.
16. Latvian State Security Service. Latest news. Available on: https://www.vdd.gov.lv/en/ Accessed June 11, 2020.
17. LETA. Mobilo sakaru operatori gatavi informēt par klientu aptuveno atrašanās vietu saistībā ar Covid-19. Available on: https://www.la.lv/mobilo-sakaru-operatori-gatavi-informet-par-klientu-aptuveno-atrasanas-vietu-saistiba-ar-covid-19 Accessed June 5, 2020.

18. Library of Congress Law. Global Legal Monitor. Netherlands: Court Strikes Down Data Retention Law. Available on: https://www.loc.gov/law/foreign-news/article/netherlands-court-strikes-down-data-retention-law/ Accessed June 7, 2020.
19. Library of Congress. European Union: ECJ Invalidates Data Retention Directive. Available on: https://www.loc.gov/law/help/eu-data-retention-directive/eu.php Accessed June 11, 2020.
20. LTV " De Facto" Arī Latvijā top mobilo telefonu rīki Covid-19 kontrolei. Ko tas nozīmē privātumam? Available on: https://www.tvnet.lv/6953512/ari-latvija-top-mobilo-telefonu-riki-covid-19-kontrolei-ko-tas-nozime-privatumam?fbclid=IwAR15yF21ykzib-gVjIzx9-DYqEmmEkewGrE4T4hdQJ1zBCZ46xwOyeNY8sA Accessed June 11, 2020.
21. Møller Pedersen, Anja, Udsen, Henrik and Sandfeld Jakobsen, Søren (2018). "Data retention In Europe—the Tele 2 case and beyond". In: International Data Privacy Law p.160.; para 14(10) Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed March 27, 2020.
22. Opinion by Emily Liu. Covid-19 has inflated racism against Asian-Americans. Here' s how to fights back. Available on: https://edition.cnn.com/2020/04/10/opinions/how-to-fight-bias-against-asian-americans-covid-19-liu/index.html Accessed June 11, 2020.
23. State Chancellery. Stricter rules for physical distancing of persons are introduced to limit the spread of Covid-19. Available on: https://www.mk.gov.lv/en/aktualitates/stricter-rules-physical-distancing-persons-are-introduced-limit-spread-covid-19 last visited on 30.03.2020. Accessed June 2, 2020.
24. Supreme Court of the United Sates, Timothy Ivory Carpenter v. United Staes, No.16-402. Available on: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf . Accessed June 11, 2020.
25. Telecommunications Industry Dialog. Provision of real-time lawful interception assistance. Available on: http://www.telecomindustrydialogue.org/resources/sweden/ Accessed May 31, 2020.
26. The Electronic Frontier Foundation. About EFF. Available on: https://www.eff.org/about Accessed June 11, 2020
27. The Ministry of Transport. Available on: http://www.sam.gov.lv/satmin/content/?cat=8 Accessed June 11, 2020.
28. The State Chancellery. Stricter rules for physical distancing of persons are introduced to limit the spread of Covid-19. Available on: https://www.mk.gov.lv/en/aktualitates/stricter-rules-physical-distancing-persons-are-introduced-limit-spread-covid-19 Accessed June 11, 2020
29. Tvnet. Sakaru operatoriem būs jāsniedz dati par Covid-19 inficēto vai to kontaktpersonu atrašanās vietu. Available on: https://www.tvnet.lv/6936296/sakaru-operatoriem-bus-

jasniedz-dati-par-covid-19-inficeto-vai-to-kontaktpersonu-atrasanas-vietu Accessed June 11, 2020.

30. Zack Doffman .COVID-19 Phone Location Trackin: Yes, It's Happening Now- Here's What You Should Know. Available on: https://www.forbes.com/sites/zakdoffman/2020/03/27/covid-19-phone-location-tracking-its-moving-fast-this-is-whats-happening-now/#48eff44611d3 Accessed March 27, 2020.

Annex 1: Letter from the Ministry of Transport

Gogoļa iela 3, Rīga, LV-1743, tālr. 67028210, fakss 67217180, e-pasts satiksmes.ministrija@sam.gov.lv, www.sam.gov.lv

Rīgā 29.04.2020 Nr. 01-13/1551

uz 06.04.2020. Nr. _____

Elvīrai Cupikai
elvira.cupika@gmail.com

Par elektronisko sakaru datu izmantošanu

Satiksmes ministrija ir saņēmusi Jūsu 2020. gada. 6. aprīļa elektroniskā pasta iesniegumu ar jautājumiem par Elektronisko sakaru likumu kontekstā ar Latvijas Universitātes (turpmāk - LU) un sabiedrības ar ierobežotu atbildību "Latvijas mobilais telefons" (turpmāk - LMT) veikto pētījumu, kas publicēts portālā "LSM.lv", un ar datu izsniegšanu Slimību profilakses un kontroles centram (turpmāk - SPKC) epidemioloģiskās izmeklēšanas veikšanai un Covid-19 ierobežošanai.

Atbildot uz pirmo jautājumu, skaidrojam, ka saskaņā ar likuma "Par valsts institūciju darbību ārkārtējās situācijas laikā saistībā ar Covid-19 izplatību" 33.pantu "Valsts policija pēc Slimību profilakses un kontroles centra lūguma pieprasa un elektronisko sakaru komersanti tai sniedz datus (telefona numurs un atrašanās vieta) par personu, kuru Slimību profilakses un kontroles centrs ir identificējis kā ar Covid-19 inficētas personas kontaktpersonu vai personu, kurai laboratoriski apstiprināta Covid-19 diagnoze. Valsts policija no elektronisko sakaru komersanta saņemtos datus nodod Slimību profilakses un kontroles centram epidemioloģiskās izmeklēšanas veikšanai".

Tādējādi, Valsts policija, saņemot SPKC pieprasījumu par konkrētu personu, saskaņā ar Ministru kabineta 2007. gada 4. decembra noteikumos Nr.820 "Kārtība, kādā pirmstiesas izmeklēšanas iestādes, operatīvās darbības subjekti, valsts drošības iestādes, Konkurences padome, prokuratūra un tiesa pieprasa un elektronisko sakaru komersants nodod saglabājamos datus, un kārtība, kādā apkopo statistisko informāciju par saglabājamo datu pieprasījumiem un to izsniegšanu" noteikto kārtību pieprasa no elektronisko sakaru komersanta konkrētus datus un pēc to saņemšanas nodod tos SPKC. Līdz ar to secināms, ka dati tiek iegūti uz likumiska pamata un tikai tādā apjomā, lai SPKC īstenotu savus pienākumus ārkārtas situācijas laikā. Vienlaikus tiek ievērota arī regulējumā nostiprinātā datu izsniegšanas kārtība.

Saistībā ar otro jautājumu Satiksmes ministrija, apzinot informāciju, ir secinājusi, ka LU un LMT pētījumā tika izmantota "mobilā tīkla notikumu statistika", citiem vārdiem – vispārīgi dati par bāzes staciju noslodzes izmaiņām pirms gada un šogad. Līdz ar to šāds detalizācijas līmenis satur tikai vispārīgu informāciju par kopējo noslodzi konkrētā bāzes stacijā un pētījums nesatur datus par identificējamu galalietotāju. Ņemot to vērā, secināms, ka pētījumā nav izmantoti dati, kuru izmantošana ir regulēta Elektronisko sakaru likumā. Tādējādi nav saskatāms Elektronisko sakaru likumā noteikto prasību par galalietotāju personas datu aizsardzību pārkāpums.

Annex 2: Letter from the State Data Inspectorate

Labdien,

Atbildot uz Jūsu 2020.gada 6.aprīļa elektroniskā pasta vēstuli informējam, ka atbildes uz Jūsu jautājumiem tiks sniegtas tādā secībā, kādā tie ir uzdoti:

1. Ziņas par personas telefona numuru un atrašanās vietu ir personas privātās dzīves sastāvdaļa. Šo datu nodošana trešajai personai neatkarīgi no nodotās informācijas tālākās izmantošanas aizskar attiecīgo personu privāto dzīvi un līdz ar to uzskatāma par privātās dzīves ierobežojumu Latvijas Republikas Satversmes 96.panta un Eiropas Cilvēka tiesību un pamatbrīvību konvencijas 8.panta izpratnē.

Kā vairākkārtīgi atzinusi Satversmes tiesa, Eiropas Cilvēktiesību tiesa un Eiropas Savienības tiesa, privātās dzīves ierobežojums attaisnojams, ja tas ir noteikts ar likumu, nepieciešams demokrātiskā sabiedrībā leģitīmu mērķu sasniegšanai un ir samērīgs ar tā mērķi.

Satversmes tiesa (2003.gada 5.jūnija spriedums lietā Nr.2003-02-0106, 2003.gada 29.oktobra spriedums lietā Nr.2003-05-01, 1999.gada 6.jūlija sprieduma lietā Nr.04-02(99) u.c.) un Latvijas Republikas Augstākā tiesa (2011.gada 12.janvāra lēmums lietā Nr.SKA–221/2011, 2010.gada 1.jūlija spriedums lietā Nr. SKA–347/2010 2007.gada 8.jūnija spriedums lietā Nr.SKA-194/2007 u.c.) norāda, ka izvērtējot, vai indivīda tiesību ierobežojums ir attaisnots, jāvērtē, vai ierobežojums ir paredzēts likumā, tas ir vērsts uz leģitīma mērķa sasniegšanu un ir nepieciešams demokrātiskā sabiedrībā, pārbaudot, vai ierobežojumi ir sociāli nepieciešami un samērīgi.

Satversmes tiesa 2010.gada 18.februāra spriedumā lietā Nr.2009-74-01 norāda, ka Satversmē noteiktās pamat tiesības var ierobežot, ja vien ierobežojums ir noteikts ar pienācīgā kārtā pieņemtu likumu, tam ir leģitīms mērķis un tas ir samērīgs. Savukārt 2011.gada 14.marta spriedumā lietā Nr.2010-51-01 Satversmes tiesa norāda, ka no starptautiskajiem cilvēktiesību aizsardzības dokumentiem vispirms izriet vispārīgie personas datu aizsardzības pamatprincipi: tiesiskums, taisnīgums, minimalitāte un anonimitāte. Šo principu kontekstā likumdevējam ir konstitucionāli noteikts pienākums pieņemt tādus tiesību aktus, kas garantētu datu drošību, kā arī noteiktu samērīgus ierobežojumus to izmantošanai.

Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 par fizisko personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (turpmāk – Regula) 6.panta 1.punktu apstrāde ir likumīga tikai tādā apmērā un tikai tad, ja ir piemērojams vismaz viens no 6.panta 1.punktā minētajiem pamatojumiem (Regulā ir noteikti seši vispārīgi tiesiskie pamati: piekrišana, līguma izpilde, juridisks pienākums, sabiedrības intereses, vitālo interešu aizsardzība un leģitīmo interešu ievērošana). Proti, tikai pastāvot kādam no minētajiem tiesiskajiem pamatiem, personas datu apstrāde tiek atzīta par tiesisku.

Jūsu 1.jautājumā minētais "sakaru operatori drīkst medicīnas darbiniekiem izsniegt Elektronisko sakaru likumā noteikto informāciju" nesniedz konkrētu informāciju, ko Jūs domājāt, minot medicīnas darbiniekus, proti, vai ir domāts ārstniecības iestāžu personāls, Slimību profilakses un kontroles centra personāls, neatliekamās medicīniskās palīdzības dienesta personāls u.c, līdz ar to Datu valsts inspekcija šobrīd nevar Jums sniegt konkrētu atbildi, vai elektronisko sakaru komersantu veikta darbība, izsniedzot medicīnas darbiniekiem Elektronisko sakaru likumā noteikto informāciju bez tiesneša akcepta, ir vērtējama kā privātuma pārkāpšana.

Vienlaikus, Datu valsts inspekcija informē, ka Elektronisko sakaru likuma 71.panta septītā daļa paredz, ka Elektronisko sakaru komersants drīkst apstrādāt atrašanās vietas datus bez lietotāja vai abonenta piekrišanas, ja atrašanās vietas datu apstrāde ir nepieciešama Valsts ugunsdzēsības un glābšanas dienestam, Valsts policijai, neatliekamās medicīniskās palīdzības un gāzes avārijas dienestiem, Jūras meklēšanas un glābšanas dienestam, kā arī Iekšlietu ministrijas Informācijas centram tā pienākumu veikšanai un šo datu nodošanai šajā panta daļā minētajiem dienestiem.

Līdz ar to neatliekamās medicīniskās palīdzības dienestam ir tiesības saņemt no elektronisko sakaru komersantiem informāciju par personu atrašanas vietu.

Tāpat, Likuma "Par valsts institūciju darbību ārkārtējās situācijas laikā saistībā ar Covid-19 izplatību" 33.pants nosaka, ka Valsts policija pēc Slimību profilakses un kontroles centra lūguma pieprasa un elektronisko sakaru komersanti tai sniedz datus (telefona numurs un atrašanās vieta) par personu, kuru Slimību profilakses un kontroles centrs ir identificējis kā ar Covid-19 inficētas personas kontaktpersonu vai personu, kurai laboratoriski apstiprināta Covid-19 diagnoze. Valsts policija no elektronisko sakaru komersanta saņemtos datus nodod Slimību profilakses un kontroles centram epidemioloģiskās izmeklēšanas veikšanai.

Līdz ar to konstatējams, ka Slimību profilakses un kontroles centrs arī tiesīgs apstrādāt informāciju, kura iegūta no elektronisko sakaru komersantiem.

Ņemot vērā iepriekš minēto, Datu valsts inspekcija paskaidro, ka abos iepriekš minētajos gadījumos, datu apstrādes tiesiskais pamats ir Regulas 6.panta 1.punkta c) apakšpunkts (apstrāde ir vajadzīga, lai izpildītu uz pārzini attiecināmu juridisku pienākumu).

2. Jūsu elektroniskā pasta vēstulē minētā publikācija Latvijas Sabiedrisko Mediju portālā neliecina, kā arī Datu valsts inspekcijas rīcībā nav informācijas, ka Mobilā tīkla pētījumā, kuru veic Latvijas Universitātes (LU) un "Latvijas Mobilā telefona" (LMT) pētnieki, tiek apstrādāti personas dati. Vēršam uzmanību, ka Elektronisko sakaru likuma 71.panta otrā daļa paredz, ka atrašanās vietas datu apstrāde citam mērķim bez lietotāja vai abonenta piekrišanas ir atļauta tādā gadījumā, ja lietotāju vai abonentu nav iespējams identificēt, izmantojot šos atrašanās vietas datus. Ņemot vērā, ka norādītajā pētījumā tiek veikta statistiskas informācijas analīze, kas nav attiecināma uz konkrētu lietotāju, kā arī Inspekcijas rīcībā nav informācijas, ka LMT un/vai Latvijas Universitāte būtu statistiskās informācijas iegūšanai apstrādājuši datus, kas attiecināmi uz identificētām vai identificējamām personām, Inspekcija pašlaik neidentificē, ka pētījums tiktu veikts pretrunā ar Elektronisko sakaru likuma nosacījumiem.

3.Savukārt attiecībā uz Jūsu jautājumu, vai Elektronisko sakaru likums nepārkāpj Eiropas Savienības Pamattiesību Hartas 7.pantu un Eiropas Cilvēktiesību 8.pantu, paskaidrojam, ka Datu valsts inspekcijas kompetenci, uzdevumus un tiesības noteic Regulas 55., 57., 58.pants un Fizisko personu datu apstrādes likuma 4. un 5.pants, kas neparedz tās tiesības vērtēt normatīvā akta atbilstību Regulai. Saskaņā ar Satversmes tiesas likuma 16.pantu Satversmes tiesa izskata lietas par citu normatīvo aktu vai to daļu atbilstību augstāka juridiska spēka tiesību normām (aktiem). Tas pats attiecināms uz šajā vēstulē iepriekš pieminēto likumu "Par valsts institūciju darbību ārkārtējās situācijas laikā saistībā ar Covid-19 izplatību".

Cieņā, Datu valsts inspekcija