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

Vera Pallasvesa

ENCRYPTION'S AND DATA PRIVACY'S RELEVANCE TO ARTICLE 34 OF THE UN CONVENTION ON THE RIGHTS OF THE CHILD

Bachelor's thesis
Programme HAJB08/17, specialisation EU and International Law

Supervisor: Thomas Hoffmann

Tallinn 2020

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 11 223 words from the introduction to the end of conclusion.

Vera Pallasvesa ……

(signature, date)

Student code: 177701HAJB
Student e-mail address: pallasvesa.vera@gmail.com

Supervisor: Thomas Hoffman:
The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:
Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

This thesis aims to examine if data privacy and encryption is violating the right provided in the Article 34 of the UN Convention on the Rights of the Child and to research the best alternatives that would support data privacy and not violate children's right to be protected from sexual exploitation. The main focus is in the European Union.

The thesis gives an overview on encryption and data privacy. An overview on the legislations regarding children will be given. It will be evaluated if law enforcement authorities have sufficient means to ensure children's protection from online sexual exploitation and what could these means be if the current ones are not sufficient enough.

The hypothesis is that there are not sufficient means to ensure that children enjoy the right provided in the Article 34(c) of the UN Convention on the Rights of the Child and that the legislation lacks proper methods to protect children from exploitation on the internet and there is a lack on the proper means to obtain the necessary evidence that is needed for the conviction of criminals. The goal is to provide the best alternative that would not violate children's rights and would support strong data privacy.

Methodology used is qualitative method. Primary sources are legislation from the European Union and the United Nations. Official papers from the Commission, Council and Europol are used. Secondary sources are articles written by legal scholars and news articles about the topic.

Keywords: encryption, end-to-end encryption, data privacy, child sexual exploitation

INTRODUCTION

The internet and technology have changed the way people communicate and brought up new possibilities in many ways for communicating and storing data. With these new possibilities comes new challenges. During recent years there have been a lot of public discussion and legislation reforms relating to data privacy having an emphasis on personal data, the use of encryption as a way to ensure data privacy and protection, and the growing problem of online child sexual exploitation. The most known legislative reform is the General Data Protection Regulation[1] that has been the center of discussion for the past couple of years. Child sexual exploitation in electronic communications has increased a lot in the recent years[2] and at the same time discussions and legislations have had a focus on increasing data privacy and starting to use encryption more widely. All of these are topical issues that are linked to each other but not necessarily having the same aim.

In this thesis the aim is to find out if the increase in data privacy and encryption is in contradiction to the aim to combat child sexual exploitation in electronic communications, especially having focus on Article 34(c) of the UN Convention on the Rights of the Child.[3] Is the increasing adoption of encryption especially by big international social networking services whose electronic communication services are used widely by people across the globe harming the protection of children form exploitation in the online environment. The focus is also on how the encrypted material has affected law enforcement authorities and what are the possible solutions that have been brought up in international discussions. The aim of the thesis is after establishing an overview of the current situation on the above-mentioned topics to research what

[1] 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),

[2] Keller M. H., Dance G. J.X., (2019) The Internet Is Overrun With Images of Child Sexual Abuse. What went wrong? *New York Times*, Retrieved from https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html, 29 April 2020

[3] United Nations, Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49

are the alternative options to achieve proper data privacy in a way that it is not violating the right of children to be protected from online sexual exploitation.

Research method used in this thesis is qualitative method. Legislation from the European Union and the United Nations is used as primary sources. Articles that are written by legal scholars are used as secondary sources. In these articles the scholars either analyze relevant issues and topics relating to this thesis or argue one side with their comments to the topic. Also, research reports and other relevant material are used.

Chapter one will introduce encryption and explain what it is and what it is used for. In this chapter an overview on the history and development of encryption is provided. The focus is on encryption in the European Union and on the discussion around it in the European Union. Chapter two will focus on data privacy giving an overview on what it is and the recent developments around it. The focus will again be on the European Union and the legislation in the European Union. Special emphasis is on the General Data Protection Regulation[4]. Chapter three will give an overview on children's rights and legislations regarding children, focusing on Article 34 of the UN Convention on the Rights of the Child[5]. The chapter will also focus on the child sexual exploitation happening online and provide an overview of the current situation regarding the topic. Chapter four focuses on the recent developments and topical discussions regarding online child sexual exploitation, data privacy and the use of encryption. It will bring out the point of view of both sides of the debate: private and legal persons favoring strong encryption and private and legal persons that have the opinion that this is harming children's rights to be protected from sexual exploitation and making law enforcement authorities struggle when trying to collect evidence and detect the exploitation happening online. Chapter five will discuss and examine the possible solutions that will ensure a satisfying level of data privacy but not harming the protection of children from online exploitation. Different alternatives are going to be discussed and evaluated to identify if a solution which would support both data privacy and protecting children from exploitation exists.

The expected outcome of this thesis is that there is not sufficient means to ensure that children enjoy the right provided in the Article 34(c) of the UN Convention on the Rights of the Child[6]

[4] Regulation (EU) 2016/679, *supra nota* 1.
[5] United Nations, Convention on the Rights of the Child, *supra nota 3*
[6] *Ibid.*

and that the legislation lacks proper methods to protect children from exploitation on the internet and there is a lack on the proper means to obtain the necessary evidence that is needed for the conviction of criminals. The goal is to be able to examine the alternative solutions for this problem that would support strong data privacy and not violate children's rights to be protected from online sexual exploitation.

This has been during recent years a discussed and controversial topic since there is a high need for data privacy and the protection of personal data. However, children's rights are very important and the question is, is the protection of personal data and data privacy gone so far that law enforcement authorities are not able to protect children from sexual exploitation that is happening online and effectively convict these criminals since the obtaining of evidence is so much more difficult when encryption is involved and how could this issue be solved so that the solution would satisfy the different parties of the debate.

1. ENCRYPTION

1.1. What is encryption?

Encryption is a way to secure data from unauthorized access. It is a technical measure to ensure cybersecurity and the protection of personal data. Encrypted data can only be accessed by a key to that specific data. Without the key the data is in an unreadable form. The process of coding data to an unreadable form using a key is called encryption and the reverse process of decoding the data using the key is called decryption. Encryption is an important technology to secure data and communication and to prevent unauthorized access. To have access to encrypted data one must know the key, otherwise the data cannot be decrypted, and this way made again available in a readable form.[7] Even though encryption is a great way to ensure cybersecurity and protect personal data it has some downsides to it. The use of encryption in criminal activity is a problem. When encryption is used in criminal activity it makes it more difficult for law enforcement authorities to obtain information that could be used as evidence in criminal investigations. The use of encryption is expected to grow in the future.[8] The use of end-to-end encryption has increased a lot within messaging since large social networking services like WhatsApp have adopted end-to-end encryption to their applications. In end-to-end encryption not even the social networking service has access to the encrypted messages.[9]

[7] Kapoor, B., Pandya, P., (2014) Data Encryption. In J. R. Vacca (Ed.) *Cyber Security and IT Infrastructure Protection*, Elsevier Science & Technology Books, ProQuest Ebook Central, 29-30; Ellis, S. R., (2009) A Cryptography Primer In J.R. Vacca (Ed.) *Computer and Information Security Handbook*, Elsevier Science & Technology, ProQuest Ebook Central. 23-24.
[8] European Commission, Migration and Home Affairs, *Encryption*. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption_en, 8 March 2020
[9] Ermoshina, K., Musiani, F., & Halpin, H. (2016). End-to-end encrypted messaging protocols: An overview. *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9934*, 244.

1.2. History and development

Encryption is not something that has been created in the modern days as pointed out in detail by Koops and Kosta. Before machine encryption was introduced in the period of First World War people had other means to encrypt messages and communicate secretly. The machines encrypted and decrypted automatically. During the Second World War machine encryption was widely used by different countries and the countries tried to crack each other's encryptions. In the 1970s encryption developed and became stronger than ever. The encryption systems were so much stronger that it was impossible to crack them like it had been before that. During the Cold War countries imposed restrictions to the export of cryptography and it was only allowed to export weak cryptography that is easily cracked and for the export of stronger cryptography a license was needed. During the 1990s it was also noticed that the use of cryptography can strongly affect law enforcement authorities. Two possible solutions were created to tackle this issue: to make sure that law enforcement authorities have the key to encrypted data beforehand or to have legislation that allows law enforcement authorities to force someone to decrypt or give the key to the encrypted data. However, these both have some flaws and the debate around encryption continued to find a solution that would help law enforcement authorities but not harm the protection of privacy. Many countries tried to make new legislations around cryptography and backdoors to ensure that law enforcement authorities would have access to the encrypted evidence but by the end of 1990s all of these new legislations were given out. The other option to gain access to encrypted data was to make the giving of the key to encrypted data to law enforcement authorities mandatory. This is also problematic since privilege against self-incrimination is a fundamental right. Because of that this option is controversial and there are not many cases published where this has been used. To get a solution if decryption orders are or are not violating fundamental rights a decision from the European Court of Human Rights is needed. However, when it comes to biometric means to decrypt data it is not as controversial because it is not linked to the will of a person.[10]

End-to-end encryption has shown to be the biggest problem. End-to-end encryption is nowadays provided for example by WhatsApp to its everyday users, so it is not something that is used only by a small portion of people that have enough knowledge and skills to end-to-end encrypt their

[10] Koops, B., Kosta, E. (2018). Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(4), 890-895

data.[11] End-to-end encryption means that not even the social networking service provider who is providing end-to-end encrypted communication can access the data.[12] As pointed out by Koops and Kosta Snowden's disclosures relating to the interception capabilities of intelligence services made people more aware of data privacy and encryption tools and this way there has been a rising use of encryption tools. Sometimes people are not even aware that their data or communication is encrypted because so many social networking service providers use encryption nowadays. The rising use of end-to-end encryption has again brought up the discussion of backdoors for law enforcement authorities. However, as stated before this is not an ideal solution since a backdoor weakens the encryption and makes possible criminal attacks more likely.[13] This was also stated in the EU Agency for Network and Information Security's and Europol's joint declaration "On lawful criminal investigation that respects 21st Century data protection".[14] ENISA also published an Opinion Paper on Encryption a few months later where it was stated that "the use of backdoors in cryptography is not a solution".[15]

The new solution that has been introduced is allowing through legislation law enforcement authorities to legally hack for example a suspect's phone to gain access to encrypted data. According to a study made for the European Parliament in 2017 these kinds of legislations are already in place or are being proposed in several EU Member States.[16]

1.3. Encryption in the European Union

In the Europol's 2016 Internet Organised Crime Threat Assessment[17] the use of encryption was mentioned in several contexts. It was recognized how the growing use of encryption among criminals is creating obstacles for law enforcement authorities to detect, investigate and to prosecute the criminal activity. This affects all crime areas. The native encryption on mobile devices was recognized to make this problem even worse. However, the importance of

[11] *Ibid.*, 896.
[12] Schultz W., Hoboken van J., (2016) *Human Rights and Encryption,* Report for UNESCO, 15.
[13] Koops, B., Kosta, E. (2018). *supra nota* 10, 896-898.
[14] ENISA, Europol, (2016) *Joint Declaration "On lawful criminal investigation that respects 21st Century data protection",* Retrieved from: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection. 30 April 2020
[15] European Union Agency For Network and Information Security, (2016) *ENISA's Opinion Paper on Encryption, Strong Encryption Safeguards our Digital Identity*, Retrieved from: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption 30 April 2020 5.
[16] Koops B., Kosta, E., (2018) *supra nota* 10. 898.
[17] Europol, (2016) IOCTA 2016, Internet Organised Crime Threat Assessment

encryption was also recognized relating to e-commerce and to activities taking place in cyberspace.

Some key threats relating to child sexual exploitation that Europol discusses in the Assessment are closely linked with encryption since for example sexual coercion that is one of the key threats is often happening on apps that are encrypted by default. Also, the access to child sexual exploitation material online has become easier and more user friendly through the expansion of tools that provide anonymization and encryption, and the offenders use encryption to avoid law enforcement authorities. The criminals also share knowledge between each other. On the other hand, when data breaches are being discussed one of the recommendations relating to them is the using of measures such as encryption to protect individuals' identities. The recommendation for a solution for the criminal communications that are happening online is that the law enforcement authorities should make sure to have enough tools, training, and tactics to get access to the necessary evidence. Overall the assessment presents several instances where encryption is playing a role to make the work of law enforcement authorities more difficult and aiding criminals. However, it is also recognized how encryption can act as a measure to protect data when needed.[18]

In May 2016 ENISA and Europol agreed that backdoors are not a solution for accessing encrypted data by law enforcement authorities since they would weaken encryption in a way that could be harmful for data privacy.[19]

There has been a lot of discussion in the EU during the recent years relating to encryption especially in criminal investigations. In September 2016 the Council concluded a questionnaire to Member States relating to encryption of data and the issues and challenges it imposes to law enforcement authorities and criminal investigations.[20] The answers were published in October 2016. The answers revealed that "encryption is encountered often or almost always in the context of criminal investigations".[21] Mostly because of the right against self-incrimination "neither the suspect, nor the accused who is in possession of a digital device/electronic data are under the

[18] Europol, (2016) *supra nota 17*

[19] Stupp, C., (2016), *EU cybersecurity and police chiefs reach breakthrough agreement on encryption*, Euractiv, Retrieved from: https://www.euractiv.com/section/digital/news/eu-cybersecurity-and-police-chiefs-reach-breakthrough-agreement-on-encryption, 25 April 2020

[20] Council of the European Union, (2016) Note from Presidency to Delegations, *Encryption of data – Questionnaire*, Retrieved from: http://data.consilium.europa.eu/doc/document/ST-12368-2016-INIT/en/pdf, 8 March 2020

[21] Council of the European Union, (2016) Note from Presidency to Delegations*, Encryption of data: Mapping of the problem – orientation debate*, Retrieved from: http://www.statewatch.org/news/2016/oct/eu-encryption-orientation-debate-13434-16.pdf, 8 March 2020, 3.

legal obligation to provide to the law enforcement authorities the encryption keys/passwords"[22] and "service providers are obliged according to national law to provide law enforcement authorities with encryption keys/passwords"[23]. The questionnaire also revealed that "the lack of sufficient technical capacity both in terms of efficient technical solutions to decrypt and respective equipment is among the top three challenges, followed by the lack of sufficient financial resources and personal capacity"[24] and that "the need for practically orientated measures prevailed over the need for adoption of new legislation on EU level"[25].

In the end of November 2016, the Presidency of the Council of the European Union made a progress report to the Permanent Representatives Committee/Council about the challenges that encryption creates to criminal justice. In the report the Presidency brought up the fact that encryption is an important tool for the protection of privacy but that it creates some problems for criminal justice. The Presidency concluded that to deal with this issue the focus should not be in new legislations and instead in policy and practical solutions.[26]

In the Joint Communication to the European Parliament and the Council on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" from 2017 it was stated that "strong encryption is the basis for secure digital identification systems that play a key role in effective cybersecurity[27]; it also keeps people's intellectual property secure and enables protecting fundamental rights such as freedom of expression and the protection of personal data, and ensures safe online commerce".[28] The Joint Communication also recognized the problem of criminals using encryption in criminal activity.[29]

---

[22] *Ibid*., 3.
[23] *Ibid*., 4.
[24] *Ibid*., 4.
[25] *Ibid*., 4.
[26] Council of the European Union, (2016) Note from Presidency to Permanent Representatives Committee/Council, *Encryption: Challenges for criminal justice in relation to the use of encryption – future steps - progress report,* Retrieved from: http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf, 25 April 2020, 5.
[27] European Commission, (2017) Joint Communication to the European Parliament and the Council, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,* Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en, 8 March 2020, 9.
[28] European Commission, (2017), Cybersecurity in the European Digital Single Market European Commission, High level group of Scientific Advisors, Retrieved from: https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf, 8 March 2020, referenced in European Commission (2017), *supra nota* 27. 9-10.
[29] European Commission (2017), *supra nota* 27, 14.

The Joint Communication was followed by the Eleventh progress report in October 2017. The goal was to identify how the use of encryption is affecting criminal investigations. In the report the Commission recognized that "the use of encryption is essential to ensure cybersecurity and the protection of personal data. EU legislation specifically notes the role of encryption in ensuring appropriate security for the processing of personal data".[30] However, the Commission stated that the use of encryption in criminal activity is a problem and has an effect on the law enforcement and judicial authorities and makes criminal investigations more demanding. It was stated that the use of encryption by criminals is expected to grow.[31] In the report there was a "set of measures to support law enforcement and judicial authorities".[32] These included "legal measures to facilitate access to encrypted evidence" and "technical measures".[33] Regarding the first measure relating to the legal framework the goal is to solve the challenges that law enforcement face when trying to access evidence to make the investigation and prosecution more effective. The technical measures include "support Europol to further develop its decryption capability", "a range of measures to support Member State authorities", "a toolbox of alternative investigation techniques", better communication between service providers and authorities, "training programmes for law enforcement and judicial authorities" and "continuous assessment of technical and legal aspects".[34]

The Regulation 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) came to force in 25th of May in 2018. Encryption is mentioned in the GDPR as an example for an "appropriate technical and organizational protection measure"[35] when it comes to the protection of personal data. The regulation does not set any standards or rules concerning encryption, it just acknowledges encryption as one measure for the protection of personal data. According to the Article 34 of the GDPR when there has been a breach on the personal data of a data subject and it results in "a high risk to the rights and freedoms of natural persons, the controller shall

[30] European Commission, (2017) Communication from the Commission to the European Parliament, the European Council and the Council, *Eleventh progress report towards an effective and genuine Security Union*, Retrieved from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf, 8 March 2020, 8.
[31] *Ibid*., 8
[32] *Ibid*., 8.
[33] *Ibid*., 8-9.
[34] *Ibid*., 9-10.
[35] Regulation (EU) 2016/679, *supra nota* 1, Art 32(1)(a)

communicate the personal data breach to the data subject without undue delay".[36] However, this is not required if "the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption."[37]

The Commission has not planned to make any legislative measures regarding encryption in the near future and it will have the focus on the practical measures to tackle the issues relating to encryption in criminal investigations.[38]

[36] *Ibid.,* Art 34(1)
[37] *Ibid.,* Art 34(3)(a)
[38] European Commission, Migration and Home Affairs, *supra nota* 8

2. DATA PRIVACY AND PROTECTION

Privacy and public accountability have been something that have raised discussions and debates. One side of the debate argues that people who are decent citizens without any criminal intentions should not have anything to hide from the public authorities[39] and the other side argues that there should be "privacy rights that limit invasions into private domains".[40]

The Charter of Fundamental Rights of the European Union sets out rights, freedoms and principles as common values respected in the European Union. Article 7 "Respect for private and family life" and Article 8 "Protection of personal data" are articles in the Charter which recognizes rights that everyone should have relating to communication and personal data. Article 7 states that "Everyone has the right to respect for his or her private and family life, home and communication" and Article 8 states that "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."[41]

It has been internationally acknowledged that the right to privacy does apply in addition to offline online.[42] Nowadays personal data can be collected in various ways and often the data subjects are not even aware of the amount of personal data that they share and that is being collected on the internet or different platforms like Facebook. A person can also be identified through an IP address even when the person is communicating in an anonymous forum. The use of CCTV cameras is also a way to collect personal data and the use of these is very common. Smartphones are also very common these days and downloading different applications to them

[39] Moore, A. (2000). Privacy and the encryption debate. *Knowledge, Technology & Policy, 12*(4), 72.
[40] *Ibid*., 72.
[41] Charter of Fundamental Rights of the European Union, 2000/C 364/01, Art 7, Art 8
[42] Jørgensen, R., & Desai, T. (2017). Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google. *Nordic Journal of Human Rights, 35*(2), 106.

can create a data privacy risk that the consumer might not be aware of.[43] Because of all of these new ways that personal data is being collected and processed there has been a rising need to ensure data privacy and protection. When it comes to children's data privacy it is especially important since children are more vulnerable than adults and they are still using the internet in many ways.[44]

2.1. Data privacy and protection in the European Union

The main legislation in the European Union concerning data privacy and protection was the Data Protection Directive which is from 1995. It is easy to say that since 1995 a lot has changed in the way personal data is being processed and technology has taken a big leap forward in its functions and in the way it is used in the present. This has brought some new challenges and people are sharing more of their personal data publicly whether they do it consciously or not. Through internet the sharing of data has also changed geographically and with just one click the data might be shared globally.[45] "The economic and social integration resulting from the functioning of the internal market has also led to a substantial increase in cross-border flows of data. To take full account of all these developments and promote the digital economy, there is a need to ensure a high level of protection of personal data, while at the same time allowing for the free movement of such data."[46]

Like stated above the original Data Protection Directive is from 1995 and needed updating taking account the developments regarding the use of personal data. The General Data Protection Regulation (GDPR) was entered into force in 2018 and replaced the Directive from 1995.[47] The next chapter will give an overview on the development of the Regulation.

[43] Klingspor, V. (2016). Why do we need data privacy? *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9580*, 85-87.
[44] Jasmontaite, L., De Hert, P. (2015). The EU, children under 13 years, and parental consent: A human rights analysis of a new, age-based bright-line for the protection of children on the Internet. *International Data Privacy Law, 5*(1), 20.
[45] European Council, Council of the European Union (2020) *Data protection reform*, Retrieved from: https://www.consilium.europa.eu/en/policies/data-protection-reform/, 20 March 2020
[46] *Ibid*.
[47] Regulation (EU) 2016/679, *Supra nota* 1

2.1.1. The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) was adopted in April 2016 and it entered into force in May 2018 and it "is the centerpiece of the reform of the EU regulatory framework for protection of personal data".[48] The GDPR replaced the Data Protection Directive from 1995 and it has many similarities with the Data Protection Directive, but the Regulation has many new provisions in it. The amendment of the Data Protection Directive was brought up already in 2003 when the Directorate General of the Commission for the Internal Market who had jurisdiction on the data protection policy making in the Commission published a report about the implementation of the Data Protection Directive. In this report the Directorate brought up some shortcomings relating to the Data Protection Directive. However, it was seen by the Commission that it was too early for any amendments. In 2007 a communication was adopted by the Commission that the Directive should not be amended. The Lisbon Treaty was entered into force in 2009 which brought constitutional changes to the legal structure of the European Union.[49] These changes included "introducing the right to data protection and a specific legal basis for data protection legislation in Article 16 of the Treaty on the Functioning of The European Union (TFEU); elimination of most aspects of the Maastricht Treaty's 'pillar' structure (meaning essentially that the same basic legal protections should apply to all types of data processing); increased oversight of and participation in data proception policy-making by the European Parliament; the elevation of the Charter of Fundamental Rights of the EU (CFR), which includes a specific right to data protection (Article 8 CFR), to constitutional status; and the obligation of the EU to accede to the European Convention on Human Rights (ECHR)".[50] In 2010 the Commission released a Communication that followed the 2007 communication that the Data Protection Directive does not meet the developments that technology and globalization brings. The Commission consulted many different sectors on the amendment of the Data Protection Directive and decided to form a new legislation relating to data protection. The final proposal for the GDPR was adopted in 2012 and it entered into the legislative procedure of the European Union that requires the agreement of the European Parliament and the Council of the EU. The final GDPR text was agreed on, on the 15th of December 2015.[51]

[48] Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., (Eds.) (2020) *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press, 2.
[49] *Ibid*., 3
[50] *Ibid*., 3
[51] *Ibid*., 3-10

The GDPR brought some changes to the old Directive from 1995. To be in accordance with the GDPR the privacy policies should be written clearly. Before the policies could be very long and difficult to understand. Businesses should also always ask for the users' consent. Consent must be freely given and inaction is not considered to be sufficient under the GDPR. Businesses are also obliged to inform the users of any transfers of data outside the European Union and inform the user if any automated decision-making is being made when processing the data. The processing of data should only be made for a defined purpose and if the data is being processed for any new purposes this should be informed to the user.[52] The business should inform the user in a case of a data breach[53] and the GDPR recognizes encryption as one method to protect the data from breaches.[54] The user has the so called "right to be forgotten" which means that the user can ask the business to delete any data that the business have of him or her. The user also has the right to see what data the business has of him or her and the right to move that data to somewhere else.[55] One important aspect of the GDPR is that the processing of personal data needs to happen on a legal ground and the legal ground for processing needs to be specified to the individual whose personal data is being processed.[56]

The GDPR brought many changes that businesses that handle personal data need to take into account in their way of doing business. It also brought some transparency on the way that personal data is being handled and people are more aware of data privacy and the fact that their data is being processed in many ways for example when using apps, even though there is still room for some improvement on the awareness aspect among users. The GDPR as a legislative reform emphasizes the EU's focus on data privacy and it does affect everyone who does business in the EU even though the business is not established in the EU. Since encryption is a way to secure personal data and the legislation puts strong emphasis on the protection of personal data, and the fines that can be imposed from any breaches are big[57] it can be assumed that the use of encryption by different businesses is growing and will grow in the future.

[52] European Commission, A new era for data protection in the EU, What changes after May 2018, Retrieved from: https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-changes_en.pdf, 10 May 2020
[53] *Ibid., 3.*
[54] Regulation (EU) 2016/679, *supra nota* 1
[55] European Commission, *supra nota* 52, 3.
[56] Bhaimia, S. (2018). The General Data Protection Regulation: The Next Generation of EU Data Protection. *Legal Information Management, 18*(1), 24.
[57] European Commission, *supra nota* 52, 3.

3. CHILDREN: LEGISLATION AND ONLINE SEXUAL EXPLOITATION

3.1. The UN Convention on the Rights of the Child

The UN Convention on the Rights of the Child was adopted and opened for signature, ratification and accession by General Assembly resolution on 20th of November 1989 and it was entered into force the 2nd of September 1990. The UN Convention on the Rights of the Child is the most widely ratified international human rights treaty in history. It is ratified by all other UN member states except by the United States which has signed the Convention. The Convention consists of 54 articles in total and the Convention should be interpreted as a whole. All the rights are equally important and linked to each other. The Convention sets out the civil, political, economic, social and cultural rights that all children everywhere are entitled to. It explains how adults and governments must work together to make sure all children can enjoy their rights which are not dependent on the child's ethnicity, gender, religion, language, abilities or any other status. The Convention has four general principles that include non-discrimination, best interest of the child, right to life survival and development and right to be heard. There are also optional protocols to the Convention which include "The Optional Protocol on the involvement of children in armed conflict", "The Optional Protocol to the Convention on the sale of children, child prostitution and child pornography" and "The Optional Protocol on a communications procedure".[58]

According to Article 34 of the UN Convention on the Rights of the Child "States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent: (a) The inducement or coercion of a child to engage in any unlawful sexual activity; (b) The exploitative use of children in prostitution or other unlawful sexual practices;

[58] Unicef United Kingdom, *How we protect children's rights with the UN Convention on the rights of the child,* Retrieved from: https://www.unicef.org.uk/what-we-do/un-convention-child-rights/ 12 March 2020

(c) The exploitative use of children in pornographic performances and materials."[59] In this thesis the focus is on the Article 34(c) and on the fact if the right provided in this Article can be met in the current situation relating to the high demand of data privacy and the rising use of encryption.

3.2. Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime was opened for signature in 2001 and it was entered into force in 2004.[60] "The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security…Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation."[61] Article 9 of the Convention discusses offences related to child pornography. Article 9(1) states that each party should establish laws and other measures to make "producing child pornography for the purpose of its distribution through a computer system", "offering or making child pornography through a computer system", "distributing or transmitting child pornography through a computer system", "procuring child pornography through a computer system for oneself of for another person" and "possessing child pornography in a computer system or on a computer-data storage medium" a criminal offence under domestic law. Child pornography is defined as being "material that visually depicts: a minor engaged in sexually explicit conduct; a person appearing to be minor engaged in sexually explicit conduct".[62]

3.3. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

The Convention on the protection of Children against Sexual Exploitation and Sexual Abuse was adopted by the Council of Europe in 2007. The Convention is also known as "the Lanzarote

[59] United Nations, Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49, art 34
[60] Council of Europe Portal, Treaty Office, Details of Treaty No. 185 Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, 7 May 2020
[61] *Ibid*.
[62] Council of Europe Convention on Cybercrime, Budapest, 23.6.2001, Art 9

Convention".[63] The objectives of the Convention are "to prevent and combat sexual exploitation and sexual abuse of children, to protect the rights of child victims and to promote national and international cooperation".[64] The Lanzarote Convention is signed by all 47 countries that are Member States of the Council of Europe. Of these 47 countries 38 has signed and ratified the Convention.[65] According to the legal factsheet made by ECPAT International the Lanzarote Convention is "the most advanced and complete legally binding international instrument on child sexual exploitation".[66] It also "criminalises sexual exploitation in a very comprehensive manner" and "promotes international cooperation in sharing information, investigating and prosecuting offenders".[67] The Convention is monitored by the Lanzarote Committee. This committee was established to monitor the effective implementation of the Convention by the State Parties. In addition to the monitoring of effective implementation, the Committee also gathers and analyses and helps the exchange of information between the states to improve the prevention of child sexual exploitation.[68]

3.4. Online child sexual exploitation

"One of the biggest online threats to children and young people concern the creation and subsequent proliferation of child abuse imagery, that is sexually explicit imagery that involves a person under the age of 18."[69] Child online exploitation is evolving constantly because of technology and because of the way it is providing new possibilities. Also, the availability of internet has been increasing around the world. In online child sexual exploitation the exploitation material is shared or searched for by using technologies that are based on the internet.[70] The victims of the exploitation are revictimized every time the material is accessed and viewed again and also the permanence of the distributed material because of the nature of internet makes the

[63] ECPAT, Legal Factsheet, The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Retrieved from: https://www.ecpat.org/wp-content/uploads/legacy/Legal%20Factsheet%20-%20Lanzarote%20Convention_0.pdf, 30 April 2020
[64] *Ibid*.
[65] *Ibid*.
[66] *Ibid*.
[67] *Ibid*.
[68] *Ibid*.
[69] Reid, A. (2009). Online protection of the child within Europe. *International Review of Law, Computers & Technology, 23*(3), 217.
[70] Steel, C. (2015). Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child Abuse & Neglect, 44*, 150-158.

victim suffer.[71] Child sexual exploitation material is shared, accessed and used in peer-to-peer networks,[72] web search engines[73] and chat rooms[74]. The material can be also shared by sexting which means that the child himself or herself sends images through text messages either to another minor or an adult.[75] From search engines Google and Microsoft have made some technical measures to their search engines to combat the problem of child sexual exploitation material on the internet.[76] Also "the online sexual exploitation of children is facilitated by websites that form virtual communities, via hyperlinks, to distribute images, videos and other material".[77] It is a real threat to children to have onlince contact with a person with sexual interest towards children. The internet also makes the distribution and accessing to child exploitation material more easier[78] and makes it possible for persons that have sexual interest towards children find other people with the same interest.[79] "Europol has identified key threats in the area of child sexual exploitation: Peer-to-peer (P2P) networks and anonymised access like Darknet networks (e.g. Tor). These computer environments remain the main platform to access child abuse material and the principal means for non-commercial distribution. These are invariably attractive for offenders and easy to use. The greater level of anonymity and the strong networking possibilities offered by hidden internet that exists beneath the "surface web" appear to make criminals more comfortable in offending and discussing their sexual interests. Live streaming of child sexual abuse. Facilitated by new technology, one trend concerns the profit-

[71] Von Weiler J., Haardt-Becker A., Schulte S., (2010) Care and treatment of child victims of child pornographic exploitation (CPE) in Germany Journal of Sexual Aggression, 16 (2), 211-222.
[72] Steel C., (2009) Child pornography in peer-to-peer networks, Child Abuse & Neglect, 33 (8), 560-568
[73] Steel C. (2009) Web-based child pornography: Quantification and qualification of demand International Journal of Digital Crime and Forensics (IJDCF), 1 (4) 58-69 referenced in Steel, C. (2015) *supra nota* 70, 150-158.
[74] Briggs, P. Simon, W.T. Simonsen, S. (2010) An exploratory study of Internet-initiated sexual offenses and the chat room sex offender: Has the Internet enabled a new typology of sex offender? Sexual Abuse: A Journal of Research and Treatment
[75] Mitchell, K.J., Finkelhor, D., Jones, L.M., Wolak, J., (2012) Prevalence and characteristics of youth sexting: A national study, Pediatrics, 129 (1) 13-20. ; Wolak, J., Finkelhor, D., (2013) Trends in arrests for technology-facilitated sex crimes with identified victims: the Third National Juvenile Online Victimization Study (NJOV-3) referenced in Steel, C. (2015). *supra nota* 70, 150-158.
[76] Watt, N., Garside, J., (2013) Google to tackle images of child sexual abuse with search and Youtube changes, The Guardian Retrieved from https://www.theguardian.com/technology/2013/nov/18/uk-us-dark-web-online-child-abuse-internet, 4.5.2020 referenced in Steel, C. (2015). *Supra nota* 70 150-158.
[77] Westlake, B., Bouchard, M. (2016). Liking and hyperlinking: Community detection in online child sexual exploitation networks. *Social Science Research, 59*, 23.
[78] Choo, K. (2008). Organised crime groups in cyberspace: A typology. *Trends in Organized Crime, 11*(3), 281-282.
[79] Choo, K.-K.R. (2009) Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences Research and public policy no. 103 Australian Institute of Criminology, Canberra ; Choo, K.-K.R., (2009) Responding to online child sexual grooming: an industry perspective, Trends Issues Crime Crim Justice, 379 1-6 referenced in Hillman, H., Hooper, C., & Choo, K. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 30*(6), 687.

driven abuse of children overseas, live in front of a camera at the request of westerners."[80] When it comes to combating cybercrime and child exploitation Europol has been active internationally and participated in many initiatives to fight child sexual exploitation happening online.[81]

The European Union has a four year policy cycle EMPCAT which goal is to take approritate measures to fight against serious international and organized crime. The current period is from 2018 until 2021 and it includes cybercrime and "combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material".[82]

According to the European Commission in 2005 an estimated one million child sexual abuse images were online, 50.000 new child abuse images are added each year and more than 70% of reported images involve children below the age of 10. The problem is that even though the images are detected and the child victim identified it is hard to remove the images from the internet permanently which means that the victim is being re-victimized because of the availability of the images online.[83]

According to New York Times the amount of reports made by the technology companies of child sexual exploitation imagery has increased dramatically. In 1998 the amount of reports was over 3,000 and over a decade later the amount was over 100,000. In 2014 the amount had gone over 1 million reports and in 2018 it was 18.4 million. These 18.4 million reports included over 45 million images and videos. These numbers show how the problem of sharing child sexual exploitation material online has been growing massively. The vast majority of the reports were made by Facebook.[84] According to the New York Times article "smartphone cameras, social media and cloud storage have allowed the images to multiply at an alarming rate".[85]

---

[80] Europol, *Child Sexual Exploitation*, Retrieved from: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation, 17 March 2020
[81] Calcara, G. (2013). The role of Interpol and Europol in the fight against cybercrime, with particular reference to the sexual exploitation of children online and child pornography. *Masaryk University Journal of Law and Technology, 7*(1), 30.
[82] Europol, *EU Policy Cycle – EMPCAT*, Retrieved from: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact, 17 March 2020
[83] European Commission, Migration and Home Affairs, *We Protect Global Alliance to End Child Sexual Exploitation Online*, Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse_en, 26 March 2020
[84] Keller M. H., Dance G. J.X., (2019) *Supra nota* 2
[85] *Ibid.*

4. DISCUSSIONS

Like discussed in the chapter "Encryption in the European Union", the European Union does not have any plans to make legislative measures regarding the topic of encryption. The measures that have been discussed in the European Union include practical measures, however the option of backdoors has been thrown out since it would potentially be too harmful for the aim of encryption to protect privacy. It is not clear what the practical measures to combat the issue of encryption in criminal investigations are in the European Union.

4.1. The United States of America

In the United States of America the discussion around encryption has been ongoing and even though the focus on this research has been in the European Union the global nature of the topic makes the discussions in the United States of America also worth mentioning especially because of the location of technology companies like Facebook that are playing a big role in this topic.

In the USA the recent discussion has been on a new act called the Earn It Act. Section 230 of the 1996 Communications Decency Act has protected technology companies from civil cases against them regarding something that persons using their platforms online are writing on the platform. This way the companies have not been liable for publications made by users on their platforms.[86] This new act that has been the center of the discussion would change that. Under the EARN IT Act the companies would not automatically be exempted from liability for their users' actions on the platforms, however they would need to earn the exemption of liability by following certain recommendations that would combat child sexual exploitation. Even though the act is focusing on child sexual exploitation it would have an impact on encryption. If the proposed act would pass and become legislation it could mean that technology companies could not use end-to-end

[86] Laslo, M., (2019) The Fight Over Section 230 – and the Internet as We Know It, Wired, Retrieved from: https://www.wired.com/story/fight-over-section-230-internet-as-we-know-it/ 30 April 2020

encryption on their platforms and earn their liability exemption at the same time.[87] According to a Wired article "this would put them in the position of either having to accept liability, undermine the protection of end-to-end encryption by adding a backdoor for law enforcement access, or avoid end-to-end encryption altogether".[88]

In 2015 in the US there was a shooting where 14 persons were killed and later the two perpetrators were killed in a shootout with the police.[89] The other perpetrator's iPhone was found but it was locked, and the law enforcement authorities did not have the technological capabilities to access the locked iPhone since it was full disk encrypted. The law enforcement authorities asked for assistance from Apple to get access to the encrypted iPhone's data. This ended up in a debate between Apple and the government since Apple refused to help access the encrypted iPhone.[90] This debate between Apple and the government was not solved since the law enforcement authorities got access to the encrypted iPhone's data with the help of a third party.[91] This case acts as a good example of the problem that encryption can create in a case of a criminal investigation. The law enforcement authorities can face a challenge when trying to obtain evidence from an encrypted device and this case shows how the technology companies are not necessarily willing to cooperate in situations like this and the law enforcement authorities need to come up with alternative solutions in order to gain access to the evidence needed.

4.2. Facebook's plans

In March 2019 Marc Zuckerberg published a blog post where he announced that Facebook will focus in the future to secure its users privacy and that it will adopt end-to-end encryption to

[87] Hay Newman, L., (2020) The EARN IT Act Is a Sneak Attack on Encryption, Wired Retrieved from: https://www.wired.com/story/earn-it-act-sneak-attack-on-encryption/ 4 May 2020
[88] *Ibid.*
[89] Schmidt M. S., Pérez-Peña R., (2015) F.B.I. Treating San Bernardino Attack as Terrorism Case, The New York Times, Retrieved from: https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html, 4 May 2020
[90] Lichtblau E., Benner K., (2016) Apple Fights Order to Unlock San Bernardino Gunman's iPhone, The New York Times, Retrieved from: https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html 4 May 2020
[91] Benner K., Lichtblau E., (2016) U.S. Says It Has Unlocked iPhone Without Apple, The New York Times, Retrieved from: https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html 4 May 2020

Facebook Messenger like it has already been adopted in WhatsApp.[92] Zuckerberg stated that "people's private communications should be secure. End-to-end encryption prevents anyone – including us – from seeing what people share on our services".[93] In his blog post Zuckerberg recognized that "there are real safety concerns to address before we can implement end-to-end encryption across all of our messaging services".[94] According to Zuckerberg Facebook will try to find appropriate solutions to detect misuse on their platforms with other means than accessing the actual messages since as stated above when using end-to-end encryption not even Facebook can access the messages.[95] However, even though Zuckerberg recognizes the downside of end-to-end encryption and the fact that misuse may happen for example when it comes to child exploitation, he sees that "working towards implementing end-to-end encryption for all private communications is the right thing to do".[96]

As a response to Zuckerberg's blog post the child rights organizations around the world signed an open letter to Zuckerberg expressing their concerns of the effect that end-to-end encrypting Facebook Messenger would have on the sexual abuse and exploitation of children and investigation of crimes.[97] In the letter the child rights organizations state that "we urge you to recognize and accept that an increased risk of child abuse being facilitated on or by Facebook is not a reasonable trade-off to make. Children should not be put in harm's way either as a result of commercial decisions or design choices. Unless demonstrably successful mitigations can be put in place, it seems likely that the consequence will be more serious and sustained sexual abuse on Facebook's virtual properties".[98] In the letter the child rights organizations present five measures that they urge Facebook to take. These five measures are investing on safety measures that would ensure that end-to-end encryption would not decrease children's safety and the ability of Facebook to detect misuse in their services, demonstrating that Facebook is willing "to embed a voluntary duty of care to protect children in…design decisions on encryption", consultation with child protection experts, governments and law enforcement authorities, agreeing on sharing "necessary data with governments and child protection experts to determine the effectiveness

[92] Zuckerberg, M., (2019) A Privacy-Focused Vision for Social Networking, Retrieved from: https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/, 29 April 2020
[93] *Ibid*.
[94] *Ibid*.
[95] *Ibid*.
[96] *Ibid*.
[97] ECPAT, (2020) ECPAT network urges Facebook to re-think encrypting Facebook Messenger, Retrieved from: https://www.ecpat.org/news/encrypting-facebook-messenger/, 29 April 2020
[98] *Ibid*.

of…mitigation strategy, and the impact that encryption has on threat behaviors" and not proceeding with the adoption of end-to-end encryption until it can be ensured that "any proposed mitigations have been fully tested, and will adequately address…concerns".[99]

The child rights organizations were not the only ones to comment on Zuckerberg's announcement about implementing end-to-end encryption to Facebook's platforms. UK, US and Australian governments' law enforcement officials sent also an open letter to Zuckerberg expressing their concerns of the impact that end-to-end encryption would have. In the letter law enforcement officials from the three governments wrote that Facebook should stop its plans to implement end-to-end encryption to all of its platforms[100] and it should instead "enable law enforcement to obtain lawful access to content in a readable and usable format".[101]

[99] *Ibid*.
[100] Crocker, A., Mullin, J., (2019) The Open Letter from the Governments of US, UK, and Australia to Facebook is An All-Out Attack on Encryption, EFF, Retrieved from: https://www.eff.org/deeplinks/2019/10/open-letter-governments-us-uk-and-australia-facebook-all-out-attack-encryption 29 April 2020
[101] Mac, R., Bernstein, J., (2019) Attorney General Bill Barr Will Ask Zuckerberg To Halt Plans For End-To-End Encryption Across Facebook's Apps, BuzzFeed News Retrieved from: https://www.buzzfeednews.com/article/ryanmac/bill-barr-facebook-letter-halt-encryption 29 April 2020

5. SOLUTIONS

The debate around encryption is not something new and possible solutions for the problem of law enforcement authorities having no access to the encrypted material and illegal activity staying undetected because using encryption have been discussed over time.

5.1. The approach in the EU

The Commission proposed six non-legislative measures to address the issue with encryption in the "Eleventh progress report towards an effective and genuine Security Union". These six measures are: "strengthen Europol's technical capabilities to deal with encryption", "establish a network of centres of expertise", "establish a toolbox of legal and technical instruments", "provide training to LEAs and the judiciary especially on encryption", "establish a forward-looking observatory" and "establish a structured dialogue with industry and with civil society organizations".[102] Like stated in the chapter "Encryption in the European Union" all of these measures are practical measures and the Commission has not planned to make any legislative measures relating to encryption in the near future. In the progress report when the technical capabilities are discussed it is stated that "measures that could weaken encryption or could have an impact on a larger or indiscriminate number of people would not be considered".[103] It is unclear what these types of technical measures that the Commission refers to could be that would not weaken encryption.

[102] European Commission, *Supra nota* 30, 9-10.
[103] *Ibid, 9.*

5.2. Different alternatives

Because the debate around encryption has been ongoing also when the use of cryptography gained popularity and when encryption became stronger many solutions for the problem of law enforcement authorities not being able to access the encrypted material has been discussed and even tried in practice. The two possible alternatives have been either to have law enforcement authorities to get access to the encryption keys beforehand or afterwards. These could mean for example having backdoor access to the encrypted material or using third parties that would have the key and then giving it to law enforcement in case of need. Backdoors are problematic since they often do not only make the access to law enforcement easier but also other actors who should not be accessing the encrypted data. The other problem is that people do not trust government at least in the US with a backdoor access to encrypted data. This means that backdoors are having a negative effect on the whole idea of using encryption: data privacy.[104] So, it can be concluded that pre-built backdoors do not provide an appropriate solution for the encryption issue. Also "requesting…companies to create a backdoor into the encrypted products they offer or to deliver the encryption keys to law enforcement agencies would defy their business model and the reason why customers choose their products over others".[105]

The other possible solution that has been discussed is a law which would allow law enforcement to command decryption. In practice this would mean that in case of an investigation the law enforcement authorities could command the suspect to decrypt the encrypted data. This has also some issues since at least in the US and in Europe there is a constitutional right against self-incrimination. This means that the suspect could deny decrypting the data based on this right. Another issue is that the suspect can easily claim that he or she has forgotten the key to the encrypted data. There are some cases where decryption orders have been contested in the courts but there is no definite answer to the issue of the right against self-incrimination before the European Court of Human Rights gives a judgement on it.[106]

One possible solution for law enforcement authorities to access encrypted data could be using surveillance measures in order "capture passwords, encryption keys, or plaintext before it is

[104] Koops, B., & Kosta, E. (2018) *supra nota* 10
[105] De Busser, E. (2016). Private Companies and the Transfer of Data to Law Enforcement Authorities: Challenges for Data Protection. *Maastricht Journal of European and Comparative Law, 23*(3), 489.
[106] Koops, B., & Kosta, E. (2018) *supra nota* 10, 894-895.

encrypted".[107] This could be obtained for example by using hidden video cameras. This solution does also have some downsides to it since to use the surveillance methods law enforcement authorities need to have prior knowledge of the suspect and the devices he or she is using. Surveillance is also difficult since law enforcement needs to have access to the device or the premises to do the surveillance and there is a risk that the measures are too intrusive, and the gathered information includes information that is not relevant or involve third parties.[108] The traditional methods might be effective in some cases but they do not provide an alternative for the whole issue of encryption since sometimes using traditional methods is not sufficient enough and the knowledge of encryption methods has been growing and being more accessible.

5.3. Legal hacking

Another solution for the problem is legal hacking. This means that governments would be legally allowed to hack encrypted data and these types of laws have been enacted in Europe already. In the case of using legal hacking minimum safeguards and requirements provided by the ECtHR in its case law should be respected.[109] The way legal hacking can be conducted is by using zero-day-vulnerabilities which are "software vulnerabilities for which no patch or fix has been publicly released".[110] Legal hacking has also raised discussion for and against and the challenge it is facing is "to satisfy the two equally important interests of fighting crime and terrorism and ensuring the public's need for secure and protected communications".[111] "Government-developed hacking tools can be leaked or stolen and subsequently used by malicious actors. And police purchases of third party exploits spur the market for privately developed hacking tools, which again may also be used for nefarious purposes."[112] It is also important to have sufficient supervision of hacking exercised by law enforcement authorities, to first approve the hacking and then supervise it.[113]

---

[107] Penney, S., Gibbs, D., Awj, N., Drouin,.(2017). Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter. *McGill Law Journal, 63*(2), 206-207.
[108] *Ibid* 206.
[109] Koops, B., & Kosta, E. (2018) *supra nota* 10, 899.
[110] *Ibid*., 899
[111] *Ibid*., 899.
[112] Penney, S., Gibbs, D., Awj, N., & Drouin, &. (2017). Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter. *McGill Law Journal, 63*(2), 214.
[113] Walden, I. (2018). 'The Sky is Falling!' – Responses to the 'Going Dark' problem. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(4), 906.

In the FBI and Apple case in the US the encrypted iPhone was hacked by a third party because Apple was not willing to help the FBI. It is argued that the fact that FBI was able to access this particular iPhone does not mean that this would be a permanent solution since it may not work on every iPhone and some phones use different operating system. Also, Apple is constantly developing their security measures and they are now aware that a third party was able to hack their system which means that they try to find this flaw to prevent this from happening again. It is also argued that using a third party to get access to the encrypted material can be very expensive since only one or a few persons can hack the encrypted material.[114]

Based on the research legal hacking would be the most appropriate solution. Using this solution law enforcement authorities would not have to rely on the social networking service providers help and could investigate by themselves. This would mean that the law enforcement authorities would need to have enough knowledge and technical solutions to conduct the hacking by themselves without needing help from a third party. The model that is followed in the European Union seems to be the best alternative and close to legal hacking as the goal is to find appropriate practical and technical solutions. This solution is not perfect and there are many things to take into account and according to the research made in this thesis the main thing is that the social networking service providers that use encryption on their platform are constantly making improvements and fixing possible flaws on the system. This means that the law enforcement would need constantly be monitoring the new technological changes and improvements made to keep up with the changes.

5.4. Aspects to be considered

It is hard to come up with a solution that would satisfy all the parties of the debate and for the law enforcement authorities to be exploiting zero-day vulnerabilities can be seen as controversial since this is something that hackers that do not have the best intentions might do as well and permitting the governments to hack people's data does sound like a inappropriate solution. However, when taking into account the bigger picture it is hard to imagine that any other solution would be as effective, since it is unlikely that in the long run the other solutions would

[114] Jacobsen, K. M. (2017). Game of phones, data isn't coming: Modern mobile operating system encryption and its chilling effect on law enforcement. *George Washington Law Review, 85*(2), 585-587.

work. A big reason for this is that the companies that use encryption in their platforms try to make the protection of data as secure as possible without the possibility of outside access. Another thing that should be considered in this context is how the criminal activity can be detected in the first place. If the criminals are using end-to-end encrypted communication and sharing child sexual exploitation material through the communication, how can this be detected in the first place so that law enforcement authorities become involved? According to a New York Times article technology companies make reports of suspected criminal activity on their platforms and Facebook was responsible for the biggest part of the reports.[115] However, according to a Guardian article many instances were left undetected by Facebook.[116] This issue is why the child rights organizations expressed their concern when Zuckerberg announced the adoption of end-to-end encryption across Facebook's platforms. To properly protect children from online sexual exploitation in addition to make sure that law enforcement authorities can access the data when necessary for an investigation emphasis should also be put in the technology companies' ability to detect criminal activity on their platforms so that it is reported to the law enforcement authorities. Zuckerberg said in his post that Facebook will develop alternative measures so that it would be able to detect possible criminal activity in its platform before adopting end-to-end encryption even though it is not able to read the end-to-end encrypted communication.[117]

[115] Dance G. J.X., Keller, M. H., (2020), An Explosion in Online Child Sex Abuse: What You Need to Know, New York Times, Retrieved from: https://www.nytimes.com/2019/09/29/us/takeaways-child-sex-abuse.html 7 May 2020
[116] Paul, K., (2020) Over 300 cases of child exploitation went unnoticed by Facebook – study, The Guardian, Retrieved from: https://www.theguardian.com/technology/2020/mar/04/facebook-child-exploitation-technology, 11 May 2020
[117] Zuckerberg, M., (2019) *supra nota 92*

CONCLUSION

This thesis aimed to examine and analyze if the high demand for data privacy and the growing use of encryption especially end-to-end encryption is harming the protection of children against sexual exploitation as provided in the Article 34 of the UN Convention on the Rights of the Child. After establishing an overview on the current situation, the aim was to study the possible alternative solutions to the issue that law enforcement authorities have regarding the use of encryption in criminal activity, in this thesis the focus of such criminal activity was in the sexual exploitation of children.

The hypothesis of this thesis was that there is not sufficient means to ensure that children enjoy the right in the Article 34(c) of the UN Convention on the Rights of the Child and that the legislation lacks proper methods to protect children from exploitation on the internet and there is a lack on the proper means to obtain the necessary evidence that is needed for convicting criminals. The research showed that this is a problem which is widely recognized not only in the European Union and the discussion around it has been ongoing especially during recent years. Encryption does not only impact the ability to protect children but also is used in other criminal activity and by terrorists. Since the issue of encryption in criminal investigations and detecting criminal activity is something that has been recognized across the globe there has also been a lot of discussions and possible legal and practical solutions have been brought up to tackle the issue.

The thesis aimed to identify and study the possible solution for this issue and the research showed that the discussion around the solutions was not something completely new, but the challenges have become greater because of the way encryption has develop and because of the adoption of end-to-end encryption. The research showed that there have been possible solutions for the issue of encryption over time and most of them have showed to have some flaws which make them not appropriate. However, it would be important that law enforcement authorities would have a well-established solution that they could rely on when encountering encryption on criminal investigations. According to the research made this would be to allow law enforcement

authorities to legally hack the encrypted device and have the technical knowledge and capability to do so.

According to the research made, the point of view that the European Union has taken regarding this issue seems to be the most effective one, which is that the focus would be in technical solutions. Using legal hacking opens the opportunity for law enforcement authorities to act independently without being dependent on the companies' help which like the FBI and Apple case showed is not something that happens easily if at all. Using legal hacking would most likely happen by using zero-day-vulnerabilities but the constant improving of systems can make this difficult since the companies are trying to fix the flaws in their systems. That is why there should be constant monitoring of the evolvement of encryption methods and techniques to keep the law enforcement authorities' knowhow up to date. Even though the focus should be mainly on improving technical capabilities, legislations that allow the law enforcement authorities to hack and supervises the conduct needs to be in place.

The issue of encryption does not only affect child sexual exploitation and it concerns all kinds of criminal acts happening or being planned online. The proposed solution for law enforcement authorities to gain access to encrypted material does not wholly solve the issue of online child sexual exploitation since there is the possibility that the criminal activity might stay undetected. To minimize this from happening the actors combatting child sexual abuse and the social networking service providers like Facebook should cooperate. Social networking service providers like Facebook should also take this problem into account when designing their systems and adopt appropriate safety and control measures. In 2018 Facebook was responsible for two thirds of the reports made by the technology companies[118] and it would be important that Facebook's among other's ability to detect the child sexual exploitation happening on their platform would be effective and that the adoption of end-to-end encryption would not happen before the companies can be sure that they can still detect the criminal activity on their platforms.

[118] Dance G. J.X., Keller, M. H., (2020), *supra nota* 115

The discussion around the topic will most likely continue in the future and the measures taken by the European Union and the US most likely will be different. One permanent solution might be difficult to create since technology is constantly evolving and the encryption methods can also be developed further. It would be great to see the different sides of the debate work more coherently and take actions together which would both ensure the protection of privacy and the protection of children from sexual exploitation happening online.

LIST OF REFERENCES

Scientific books

1. Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., (Eds.) (2020) *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press.

Scientific articles

2. Bhaimia, S. (2018). The General Data Protection Regulation: The Next Generation of EU Data Protection. *Legal Information Management, 18*(1), 21-28.
3. Briggs, P., Simon, W.T., Simonsen, S., (2010) An exploratory study of Internet-initiated sexual offenses and the chat room sex offender: Has the Internet enabled a new typology of sex offender? *Sexual Abuse: A Journal of Research and Treatment,* 72-91.
4. Calcara, G., (2013). The role of Interpol and Europol in the fight against cybercrime, with particular reference to the sexual exploitation of children online and child pornography. *Masaryk University Journal of Law and Technology, 7*(1), 19-33.
5. Choo, K. (2008). Organised crime groups in cyberspace: A typology. *Trends in Organized Crime, 11*(3), 270-295.
6. De Busser, E. (2016). Private Companies and the Transfer of Data to Law Enforcement Authorities: Challenges for Data Protection. *Maastricht Journal of European and Comparative Law, 23*(3), 478-494.
7. Ellis, S. R., (2009) A Cryptography Primer In J.R. Vacca (Ed.) *Computer and Information Security Handbook*, (23-38) Elsevier Science & Technology, ProQuest Ebook Central. 23-38
8. Ermoshina, K., Musiani, F., Halpin, H. (2016). End-to-end encrypted messaging protocols: An overview. *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9934*, 244-254.
9. Hillman, H., Hooper, C., Choo, K. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 30*(6), 687-698.
10. Jacobsen, K. M. (2017). Game of phones, data isn't coming: Modern mobile operating system encryption and its chilling effect on law enforcement. *George Washington Law Review, 85*(2), 566-612.

11. Jasmontaite, L., & De Hert, P. (2015). The EU, children under 13 years, and parental consent: A human rights analysis of a new, age-based bright-line for the protection of children on the Internet. *International Data Privacy Law, 5*(1), 20-33.
12. Jørgensen, R., Desai, T. (2017). Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google. *Nordic Journal of Human Rights, 35*(2), 106-126.
13. Kapoor, B., Pandya, P., (2014) Data Encryption. In J. R. Vacca (Ed.) *Cyber Security and IT Infrastructure Protection*, (29-73) Elsevier Science & Technology Books, ProQuest Ebook Central
14. Klingspor, V. (2016). Why do we need data privacy? *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9580*, 85-95.
15. Koops, B., & Kosta, E. (2018). Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(4), 890-900.
16. Moore, A. (2000). Privacy and the encryption debate. *Knowledge, Technology & Policy, 12*(4), 72-84.
17. Penney, S., Gibbs, D., Awj, N., Drouin (2017). Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter. *McGill Law Journal, 63*(2), 201-245.
18. Reid, A. (2009). Online protection of the child within Europe. *International Review of Law, Computers & Technology, 23*(3), 217-230.
19. Steel, C. (2009) Child pornography in peer-to-peer networks Child Abuse & Neglect, 33 (8), 560-568.
20. Steel, C. (2015). Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child Abuse & Neglect, 44*, 150-158.
21. Von Weiler J, Haardt-Becker, A., Schulte S., (2010) Care and treatment of child victims of child pornographic exploitation (CPE) in Germany. *Journal of Sexual Aggression*, 16 (2) 211-222.
22. Walden, I. (2018). 'The Sky is Falling!' – Responses to the 'Going Dark' problem. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(4), 901-907.
23. Westlake, B., Bouchard, M. (2016). Liking and hyperlinking: Community detection in online child sexual exploitation networks. *Social Science Research, 59*, 23-36.

EU and International legislation

24. Charter of Fundamental Rights of the European Union, 2000/C 364/01
25. Council of Europe Convention on Cybercrime, Budapest, 23.6.2001
26. 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)
27. United Nations, Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49

Other sources

28. Benner K., Lichtblau E., (2016, March 28) U.S. Says It Has Unlocked iPhone Without Apple, *The New York Times,* Retrieved from: https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html, 4.5.2020
29. Council of Europe Portal, Treaty Office, *Details of Treaty No. 185 Convention on Cybercrime*, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, 7.5.2020
30. Council of the European Union, (2016) Note from Presidency to Delegations, *Encryption of data – Questionnaire*, Retrieved from: http://data.consilium.europa.eu/doc/document/ST-12368-2016-INIT/en/pdf, 8 March 2020
31. Council of the European Union, (2016) Note from Presidency to Permanent Representatives Committee/Council, *Encryption: Challenges for criminal justice in relation to the use of encryption – future steps - progress report,* Retrieved from: http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf, 25 April 2020
32. aCrocker, A., Mullin, J., (2019, October 3) The Open Letter from the Governments of US, UK, and Australia to Facebook is An All-Out Attack on Encryption, *EFF,* Retrieved from:

https://www.eff.org/deeplinks/2019/10/open-letter-governments-us-uk-and-australia-facebook-all-out-attack-encryption 29.4.2020

33. Dance G. J.X., Keller, M. H., (2020, September 29), An Explosion in Online Child Sex Abuse: What You Need to Know, *New York Times*, Retrieved from: https://www.nytimes.com/2019/09/29/us/takeaways-child-sex-abuse.html 7.5.2020
34. ECPAT, (2020) *ECPAT network urges Facebook to re-think encrypting Facebook Messenger,* Retrieved from: https://www.ecpat.org/news/encrypting-facebook-messenger/, 29.4.2020
35. ECPAT, *Legal Factsheet, The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, Retrieved from: https://www.ecpat.org/wp-content/uploads/legacy/Legal%20Factsheet%20-%20Lanzarote%20Convention_0.pdf, 30.4.2020
36. ENISA, Europol, (2016) *Joint Declaration "On lawful criminal investigation that respects 21st Century data protection",* Retrieved from: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection. 30.4.2020
37. European Commission, (2017) Joint Communication to the European Parliament and the Council, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,* Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en, 8 March 2020
38. European Commission, (2017), Cybersecurity in the European Digital Single Market European Commission, High level group of Scientific Advisors, Retrieved from: https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf, 8 March 2020
39. European Commission, A new era for data protection in the EU, What changes after May 2018, Retrieved from: https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-changes_en.pdf
40. European Commission, Communication from the Commission to the European Parliament, the European Council and the Council (2017) *Eleventh progress report towards an effective and genuine Security Union*, Retrieved from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf, 8 March 2020

41. European Commission, Migration and Home Affairs, *Encryption*. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption_en, 8.3.2020
42. European Commission, Migration and Home Affairs, *We Protect Global Alliance to End Child Sexual Exploitation Online*, Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse_en, 26 March 2020
43. European Council, Council of the European Union (2020) *Data protection reform*, Retrieved from: https://www.consilium.europa.eu/en/policies/data-protection-reform/, 20 March 2020
44. European Union Agency For Network and Information Security, (2016) *ENISA's Opinion Paper on Encryption, Strong Encryption Safeguards our Digital Identity*, Retrieved from: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption 30.4.2020, 5.
45. Europol, (2016) IOCTA 2016, Internet Organised Crime Threat Assessment
46. Europol, *Child Sexual Exploitation*, Retrieved from: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation, 17.3.2020
47. Europol, *EU Policy Cycle – EMPCAT*, Retrieved from: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact, 17.3.2020
48. Hay Newman, L., (2020, May 3) The EARN IT Act Is a Sneak Attack on Encryption, *Wired* Retrieved from: https://www.wired.com/story/earn-it-act-sneak-attack-on-encryption/ 4.5.2020
49. Keller M. H., Dance G. J.X., (2019, September 29) The Internet Is Overrun With Images of Child Sexual Abuse. What went wrong? *New York Times*, Retrieved from https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html, 29.4.2020
50. Laslo, M., (2019, August 13) The Fight Over Section 230 – and the Internet as We Know It, *Wired,* Retrieved from: https://www.wired.com/story/fight-over-section-230-internet-as-we-know-it/ 30.4.2020
51. Lichtblau E., Benner K., (2016, February 17) Apple Fights Order to Unlock San Bernardino Gunman's iPhone, *The New York Times,* Retrieved from: https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html 4.5.2020

52. Mitchell, K.J., Finkelhor, D., Jones, L.M., Wolak, J., (2012) *Prevalence and characteristics of youth sexting: A national study*, Pediatrics, 129 (1) 13-20
53. Paul, K., (2020, March 4) Over 300 cases of child exploitation went unnoticed by Facebook – study, The Guardian, Retrieved from: https://www.theguardian.com/technology/2020/mar/04/facebook-child-exploitation-technology, 11.5.2020
54. Schmidt M. S., Pérez-Peña R., (2015, December 4) F.B.I. Treating San Bernardino Attack as Terrorism Case, *The New York Times*, Retrieved from: https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html, 4.5.2020
55. Schultz W., Hoboken van J., (2016) *Human Rights and Encryption,* Report for UNESCO, 15.
56. Stupp, C., (2016, May 20), *EU cybersecurity and police chiefs reach breakthrough agreement on encryption*, Euractiv, Retrieved from: https://www.euractiv.com/section/digital/news/eu-cybersecurity-and-police-chiefs-reach-breakthrough-agreement-on-encryption, 25 April 2020
57. Unicef United Kingdom, *How we protect children's rights with the UN Convention on the rights of the child,* Retrieved from: https://www.unicef.org.uk/what-we-do/un-convention-child-rights/ 12 March 2020
58. Watt, N., Garside, J., (2013, November 18) Google to tackle images of child sexual abuse with search and Youtube changes, *The Guardian*, Retrieved from https://www.theguardian.com/technology/2013/nov/18/uk-us-dark-web-online-child-abuse-internet, 4.5.2020
59. Zuckerberg, M., (2019, March 6) A Privacy-Focused Vision for Social Networking, Retrieved from: https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/, 29.4.2020

APPENDICES

Appendix 1. Non-exclusive licence

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

I ____Vera Pallasvesa_____(author's name)

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

_____Encryption's and Data Privacy's Relevance to Article 34 of the UN Convention on the Rights of the Child_____
_____ ,
(title of the graduation thesis)

Thomas Hoffmann
supervised by _____ ,
(supervisor's name)

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

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

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

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

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