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

Jaanika Minnus

CYBER VIOLENCE IN ESTONIA

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

Supervisor: Agnes Kasper, PhD

Tallinn 2019

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 10608 words from the introduction to the end of conclusion.

Jaanika Minnus ……

(signature, date)

Student code: 164921HAJB

Student e-mail address: jaanikaminnus@mail.ee

Supervisor: Agnes Kasper, PhD:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

"What is your Instagram? I will follow you!" is probably a question almost every youth has come across to. We are living in a digital age where likes, subscriptions and follower counts can be more important than thinking twice before posting something online. True, it does matter when being an online personality is a career and money is earned, but safety is always first. Digital world exposes people to many shapes of cyber violence. As a growing problem it needs social awareness and clear laws from the state to protect the potential victims.

The aim of this bachelor thesis is to find legal gaps in Estonian laws addressing cyber violence and provide suggestions for improvement. Conceptual analysis is chosen for the methods including legal interpretation of legislative instruments. The author states that the regulatory framework addressing cyber violence is fragmented and requires consolidation. Two questions have raised in order to check the validity of the posed hypothesis. First question inquires what gaps are found in the legal regulation towards cyber violence in Estonia and second, how to improve the legal framework regards the issue. For the first question, relevant laws are observed to analyse what is covered and to what extent by those documents. Estonian Penal Code is compared to two other European Union countries' Criminal Code to check how cyber violence is handled abroad. As to the second imposed question, the author gives recommendations on fulfilling the gaps found in the legal framework.

Keywords: Cyber Violence, Penal Code, Social Network, Cyberbullying, Internet Technology

INTRODUCTION

Times have changed drastically, because the Internet today is accessible to everybody from everywhere. There are many social media platforms being used on a daily basis for various reasons. Some users work as bloggers, influencers, YouTube personalities or Instagram models. However, companies have recently started to use social media such as Facebook, Twitter and other platforms in their workplace as well for a fast communication tool. Creation of online identities is very popular among people which is growing rapidly. In accordance, it is difficult to keep up with technologies and applications due to their constant change like with fashion.[1] Companies are working daily on their devices or programs to give consumers the best experience. People are constantly connected to the web whether from a computer, tablet or smartphone. In every second, messages are being sent, photos shared and thoughts commented. Hence, it seems that we are living in a digital age.

Internet gives a lot of power, which is often seen as dangerous and complicated to balance.[2] Cyber threats can easily occur due to massive use of technology and previously mentioned online identities. People expose their lives on the web without even thinking of the risks it imposes or they are unaware of the seriousness. Cyber violence can be seen in bullying, stalking, lying or even in identify thefts. Furthermore, the Internet has created an environment perfect for harmful activities.[3] Cyber violence is active – neither does it depend on country nor has a specific occurring time. Every person online can face such aggressive behaviour regardless the location. Therefore, the awareness of the various forms of these threats is essential to stay safe online due to virtual world's rapid growth.

The Council of Europe has conducted a study in many states regards cyber violence, but in case of Estonia, the legal framework was missed.[4] Indeed, Estonia does not have one particular document that can solely regulate cyber violence. It might cause confusion at a first glance. Currently there are several legal documents referring to social media, data protection and information services. However, these may not specific enough to reduce or regulate the problem. Maybe the problem is new to the

[1] Subrahmanyam, K., Šmahel, D. (2010). *Digital Youth: The Role of Media in Digital Development*. New York: Springer, p. 19.
[2] Savin, A. (2013). *EU Internet Law.* Cheltenham, Gloucestershire: Edward Elgar Publishing Inc., p. 1.
[3] Wall, D. (2001). *Crime and the Internet.* England: Routledge, p. 3.
[4] T-CY Mapping Study on Cyberviolence 2018.

society and the state is just starting to work on corresponding regulations. Laws addressing cyber violence need to be clear and understandable. The author chose this topic for her bachelor thesis to examine the legal framework for determining which laws are applicable in case of cyber violence. In addition, Estonian online habits are observed to be aware of the amount of people that might face those violations due to the excessive use of technologies. Estonia needs to have understandable laws related to cyber violence for two reasons: a) prevention; and b) consequences in case of infringement.

Thus, the aim is to find legal gaps in Estonian laws relating to cyber violence and provide suggestions for development. The author has given a hypothesis together with two important questions which help to determine its validity in a conclusion of this paper. The posed hypothesis is that the regulatory framework addressing cyber violence is fragmented and requires consolidation. Questions asked for support are the following:

1. What legal gaps are found in the legal regulation of cyber violence in Estonia?
2. How to improve the legal framework addressing cyber violence?

The author uses conceptual analysis as critically evaluating the possibility of harmonisation in this field. It is examined how Estonian laws regulate forms of cyber violence and to what extent. Furthermore, legal interpretation of legislative instruments and case-law analysis are used for illustration. Estonian laws are compared to two other countries, Spain and Finland to demonstrate how different countries react on the same issue.

Thesis is divided into five chapters. First chapter defines cyber violence. The beginning provides most popular types of cyber violence, since there are many varieties occurring online. In addition, it gives general understanding of the named forms by explaining the meaning of each type. Second chapter brings Estonian context where cyber violence may take place and shows dependence of the society on using internet on a daily basis. Different age groups are mentioned. Moreover, it mentions the steps the state has taken to improve the situation. Third chapter looks at the legal framework of Estonia, what laws are most relevantly used in case of cyber violence. It examines the Constitution and Penal Code, because some offences might not be criminalised. Provisions that apply the best to the definitions of the cyber violence types are analysed. The legal gaps found in legislation are stated

accordingly. Lastly, case study from the Estonian court is provided to illustrates how the case was handled and what the court should have done differently.

Fourth chapter compares Estonia to two other European countries – Finland and Spain. Finland is chosen as being its close neighbour. Spain has a constitutional monarchy while Estonia has a parliamentary republic system. Comparison will show if different governments affect the laws as well. Fifth chapter presents recommendations given by the author on how to find threshold of tolerable behaviour. These are drawn in accordance with the findings and current situation. Apart from that, it is declared how to improve the security of cyberspace in the digital age. The final part concludes the topic of this bachelor thesis. Validity of the posed hypothesis is checked and evaluated. Answers are given to the two raised questions. The author provides recommendations for further research purposes.

1. CONCEPT OF CYBER VIOLENCE

This chapter gives an overview of the popular categories of cyber violence.

1.1. Defining cyber violence

Cyber violence is an aggressive behaviour with an intent to harass.[5] It concerns mostly vulnerable groups of the society: women and girls.[6] There are many definitions to cyber violence and European Institute for Gender Equality explains the reason behind. European Union lacks an interpretation which would be known for everybody.[7] They add that countries understand and handle it differently.[8] The author wants to find out how Estonia acts regards cyber violence.

It is said that cyberspace develops all the time.[9] This reflects how broad cyber violence can be due to happening online and why there is a necessity for protection. Council of Europe reported that such violations can be found in domestic legislation.[10] Estonia does not have particular laws in one place towards cyber violence: one has to look through many legal documents and find applicable provisions. It needs attention, because people share their lifestyles on the Internet, so users are easily accessible to cybercriminals. Moreover, smart devices help them to cross limitations, even geographical.[11]

According to David S. Wall, the assault can affect mental health in a long term.[12] By his statement, the harmfulness seems to be same like in case with physical violence, because both have a similar

[5] Slaninova, G., Haviger, J., Novotna, L., Sochorova, P., Vackova, M. (2011). Relationship between cyberbullying and readiness for aggressive behavior in middle adolescence – *Procedia – Social and Behavioral Sciences*, Vol. 29, 567-573, p. 568.
[6] Cyber violence is a growing threat, especially for women and girls. *EIGE.* Accessible: https://eige.europa.eu/news/cyber-violence-growing-threat-especially-women-and-girls , 7 May 2019.
[7] *Ibid.*
[8] *Ibid.*
[9] Singer, P. W., Friedman, A. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press, p. 14.
[10] T-CY Mapping Study on Cyberviolence (2018), *supra nota* 4, p. 5.
[11] Al-Alosi, H. (2017). Cyber-violence: Digital Abuse in the Context of Domestic Violence. – *University of New South Wales Law Journal*, Vol. 40, No. 4, 1573-1603, p. 1578.
[12] Wall, D. S. (2005). The Internet as a Conduit for Criminals. – *Information Technology and the Criminal Justice System.* (Ed.) Pattavina, A. Thousand Oaks, CA: Sage Publications, 77-98, p. 84.

outcome. Nevertheless, it is unknown if those people bully online too.[13] Cyber violence can be seen all over due to previously mentioned private data reveal. What is once shared or done on the Internet also stays there, because permanent deletion is not guaranteed – a trace or mark will always remain. The more information people share about themselves, the more exposed they become.

1.2. Cyberbullying

Cyberbullying means bullying online with the help of technologies.[14] Nowadays, many concerns are about hatred anonymous comments on YouTube videos since the platform has accepted a regarding policy for controlling.[15] It would help a lot, because due to that, users are able to report the negative content they have received from viewers. Besides, bullying can also occur within online games. In 2016, there was a Blue Whale game triggering people to commit self-harm and lastly a suicide.[16]

There are more methods how offenders use their devices for targeting people. Generally, it is done by sending emails or an SMS, but it can also involve media content. [17] Intention to harm is significant in the performance.[18] Cyberbullying's miscellaneous forms are explained in further subchapters. The phenomenon needs as much attention as traditional bullying. The importance to deal with such problems should not be lowered due to happening online.

1.3. Cyberstalking

Cyberstalking is another serious violation towards people. It is a repetitious activity with the use of technology to threaten.[19] Offenders scare targets with victims' personal data or send continuous

[13] Peterson, J., Densley, J. (2017). Cyber Violence: What Do We Know and Where Do We Go from Here? – *Aggression and Violent Behavior,* Vol. 34, 193-200, p. 194.
[14] *Bullying.* Council of Europe. Acessible: https://www.coe.int/en/web/children/bullying , 23 January 2019.
[15] *Harassment and cyberbullying policy*. YouTube. Accessible: https://support.google.com/youtube/answer/2802268?hl=en , 23 January 2019.
[16] Rossow, A. (2018). *Cyberbullying Taken to a Whole New Level: Enter the 'Blue Whale Challenge'.* Accessible: https://www.forbes.com/sites/andrewrossow/2018/02/28/cyberbullying-taken-to-a-whole-new-level-enter-the-blue-whale-challenge/#177f02d82673 , 23 January 2019.
[17] Kowalski, R. M, Limber, S. P., Agatston, P. W. (2012). *Cyberbullying: Bullying in the Digital Age.* 2nd. ed. USA: Wiley-Blackwell, p. 1.
[18] T-CY Mapping Study on Cyberviolence (2018), *supra nota* 4, p. 8.
[19] Dempsey, J. S. (2010). *Introduction to Private Security.* 2nd ed. USA: Cengage Learning Inc., p. 283.

intimidating messages.[20] It may be a severe infringement towards anyone due to occurring online. With that being said, cyberstalking can extend to child abusers.[21] Digital world makes offences powerful in a way that potential victims are more reachable, because offenders have the option to stay hidden by creating fake profiles for stalking. However, Council of Europe adds in its report that even intimate partners act like that.[22]

1.4. Cyber harassment

Cyber harassment is a term for a continuous attack at a person with messages.[23] The behaviour could also involve sexual targeting since it is similar to the definition of cyberstalking as seen above. Therefore, that type of violence involves grownups rather than minors. Adults are more likely to use the action in a sexual manner since children simply bully and might not think that way early on. Different network providers have started to use methods to fight cyber harassments in social media.[24] This offers user-friendly experience. Some of the provided methods to counter the problem can be improvement of terms and conditions, age limits to certain websites and data collecting. For instance, Facebook requires people to be at least 13 of age when signing up.[25]

1.5. Outing

Outing means sharing someone's personal information on the Internet without owner's permission.[26] For example, it could be data about phone numbers, home addresses or family life. According to the Council of Europe's report, this behaviour can be a part of cyberbullying.[27] The harm is often

[20] Marcum, C. D., Higgins, G. E., Ricketts, M. L. (2014). Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration – *International Journal of Cyber Criminology*, Vol 8, No. 1, 47-56, p. 48.
[21] Hickey, E. W. (2013). *Serial Murderers and their Victims.* 6th ed. USA: Cengage Learning Inc., p. 244.
[22] T-CY Mapping Study on Cyberviolence (2018), *supra nota* 4, p. 10-11.
[23] Betts, L. (2016). *Cyberbullying: Approaches, Consequences and Interventions*. London: Palgrave Macmillan Limited, p. 19.
[24] van Laer, T. (2014). The Means to Justify the End: Combating Cyber Harassment in Social Media. – *Journal of Business Ethics*, Vol. 123, No. 1, 85-98, p. 87.
[25] *How Do I Report a Child Under the Age of 13?* Facebook Help Center. Accessible: https://www.facebook.com/help/157793540954833 , 23 April 2019.
[26] Bauman, S. (2014). *Cyberbullying: What Counselors Need to Know.* USA: John Wiley & Sons, p. 55.
[27] T-CY Mapping Study on Cyberviolence (2018), *supra nota* 4, p. 7.

significant, because it is not always easy to remove what is put online. Another similar behaviour is doxing. This also means looking for information and broadcasting it.[28]

1.6. Catfishing

This is a new term in the digital world and might not be recognisable promptly after being asked what does it mean. It started from 2012 with MTV series called 'Catfish: The TV Show' where Nev Schulman brings together online friends who have never met for some reason.[29] Estonia has aired the show too. Catfishing means building a new digital identity for oneself by using other person's photos or information.[30] It is more or less comparable to taking over someone's life and habits. Identity theft is a more known definition to such activity since the other one is modernised, but the outcome is the same.

1.7. Defamation

Defamation is considered as an untrue statement about someone that lowers the reputation of the person.[31] The written assault is called libel whilst slander is done verbally.[32] According to this interpretation, it can be assumed it is like fake news, gossip or anonymous comments.

1.8. Sexting/sextortion

Sexting is primarily a performance where a person is sending explicit text messages online including provocative content.[33] Therefore, it can be assumed when this occurs between adults as a part of dating, sexting may be more or less acceptable. If children are involved in such behaviour, it can cause

[28] *Ibid.*
[29] *Catfish: The TV Show. About the Show.* MTV UK. Accessible: http://www.mtv.co.uk/catfish-the-tv-show , 24 January 2019.
[30] *Catfishing.* The Cybersmile Foundation. Accessible: https://www.cybersmile.org/what-we-do/advice-help/catfishing , 24 January 2019.
[31] Reuvid, J. (2010). *Managing Business Risk: A Practical Guide to Protecting Your Business*. 7th. ed. UK: Kogan Page, p. 87.
[32] *Ibid.*
[33] Gillespie, A. A. (2013). Adolescents, Sexting and Human Rights. – *Human Rights Law Review,* Vol. 13, No. 4, 623-643, p. 624.

serious infringements towards them due to child pornography. Sexting may even issue problems with copyright.[34]

Sextortion is a form of blackmailing, but sexually. Offenders manipulate and create fake personalities to ask for nude photos of the victim.[35] If the person disagrees with the afterwards claim, any shared explicit content will be revealed.[36] However, sextortion demand letters can often be a scam. For instance, Estonian police has constantly announced fake email spreads where it is promised to expose sensitive media collected through specific software the receiver has no idea about.[37] Revenge porn is a part of cyber violence overlapping with sextortion. It has been defined as "the non-consensual distribution of private, sexual images by a malicious ex-partner."[38]

These types of cyber violence cases may not be taken as seriously at first, because it can be thought that someone is just playing around. Especially when it comes to sexting. Nevertheless, the behaviour should not be fully ignored since a simple text can become a criminal offence.

[34] Svantesson, D. J. B. (2011). "Sexting" and the Law – 15 Minutes of Fame, and a Lifetime of Shame – *Masaryk University Journal of Law and Technology*, Vol. 5, No. 2, 289-303, p. 289.
[35] Sciandra, M. (2017). *Cybercrime: Using Computers as Weapons*. USA: Greenhaven Publishing LLC, p. 25.
[36] *Ibid.*
[37] Mandri, J-M. (2018). *Järjekordne laine petukirjasid: RIA hoiatab sextortion-väljapressijate eest.* Accessible: http://forte.delfi.ee/news/digi/jarjekordne-laine-petukirjasid-ria-hoiatab-sextortion-valjapressijate-eest?id=83877899 , 24 January 2019.
[38] McGlynn, C., Rackley, E., Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse – *Feminist Legal Studies*, Vol. 25, No. 1, 25-46, p. 26.

2. ESTONIAN ONLINE HABITS

It is clear that smartphones make it easy for people to use cellular data instead of turning on the computer or a laptop to do a search. Almost everything can be done on phones, especially quick googling or instant messaging. According to the Statistics Estonia's quarterly bulletin, the number of Internet users on smartphones in Estonia rises all the time. To be exact, the surveys have found that 90% of citizens are using the Internet on a daily basis while 85% prefer a computer.[39] Such large numbers show red flags, because the bigger the numbers, the bigger the risks to get affected by cyber violence. Moreover, people who were interviewed ranged from 16 to 74 years[40], which means the age does not matter who are being online. Everybody has a right to use devices and Internet connection. Old people can be tricked, because of lack of knowledge about cybercrimes.[41] Therefore, they could easily fall for previously mentioned blackmailing case in the subchapter 1.8., where a sender tries to get money from the victim by threatening with sensitive data leak or passwords.

Apart from Statistics Estonia, the country participates in many other researches and surveys related to Internet usage among youth or people generally. One of those determined that children already start with devices at the age of 8.[42] Therefore, it is essential to have strong safeguards from early on in addition to improved laws regarding cyber violence. Like previously explained in related chapter, children suffer mostly from cyberbullying and it does not differ in Estonia. EU Kids Estonia had a recent survey about minors showing that 40% of participants have suffered from cyber violence.[43]

[39] Statistics Estonia. (2018). Quarterly Bulletin of Statistics Estonia. An overview of social and economic developments in Estonia 2/2018. – [E-database] https://www.stat.ee/publication-2018_quarterly-bulletin-of-statistics-estonia-2-18 (10 October 2018).
[40] *Ibid.*
[41] Arfi, N., Agarwal, S. (2013). *Knowledge of Cybercrime among Elderly*. Accessible: https://www.researchgate.net/publication/242654499_Knowledge_of_Cybercrime_among_Elderly , 25 January 2019.
[42] Kalmus, V. (2011). Ülevaade EU Kids Online Uuringu tulemustest. – *Turvalisuse interneti päeva konverents,* 11 February 2011 Tallinn. Tartu: University of Tartu.
[43] Sukk, M., Soo, K. (2018). Preliminary findings of the EU Kids Online 2018 Estonian survey: Summary. – *EU Kids Online Estonia*. (Eds). Kalmus, V., Kurvits, R., Siibak, A. Tartu: University of Tartu, Institute of Social Studies, 1-8, p. 6.

Birgy Lorenz, an expert of digital security, reveals that more than 5000 cases concerning cyber violence have been filed to the Estonian police in 2015.[44] This number could become even bigger over the years, since right now the society is more in the digital age than four years ago. The survey also found 11% of children have faced sexting[45], i.e. sending nudity texts. This kind of behaviour is strongly prohibited and needs attention, because it involves minors. In addition, Statistics Estonia's blog brought out the habits of youth in the digital world in 2017. At that time, 97% of youth had used mostly Facebook while emails were quite popular (96%)[46]. Estonia being the e-country where almost everything is digitalised could be vulnerable and a key to cyber violence if not used carefully. For example, health care data, voting system as well as online banking are also accessible with an ID-card.

State has started to take more steps towards safer cyberspace. Minister of Education and Research has said that since Estonia is innovative in the digital field, it is also needed to be aware of the fact bullying has gone viral, so the prevention is highly essential.[47] One of the successful projects is the program 'Smartly on the Web'. It helps to decrease cyber violence by giving guidelines and it declares that children are especially protected from sexting-sextortion.[48]

[44] Pealinn. (2016). *LIGI 3000 KIUSAMISJUHTU: Küberkiusamine on Eestis terav probleem, ütlevad veebikonstaablid.* Accessible: http://www.pealinn.ee/koik-uudised/ligi-3000-kiusamisjuhtu-kuberkiusamine-on-eestis-terav-probleem-n163144 , 25 January 2019.
[45] Sukk, M., Soo, K. (2018), *supra nota* 43, p. 5.
[46] Tiitsmaa, S. (2017) *Noored IT-seadmete ja interneti maailmas.* Accessible: https://blog.stat.ee/2017/10/26/noored-it-seadmete-ja-interneti-maailmas/?highlight=internet , 25 January 2019.
[47] *Minister Mailis Reps: küberkiusamise ennetamine on turvalise koolitee osa.* Haridus- ja Teadusministeerium. Accessible: https://www.hm.ee/et/uudised/minister-mailis-reps-kuberkiusamise-ennetamine-turvalise-koolitee-osa , 25 January 2019.
[48] *About the Project.* Targalt Internetis. Accessible: https://www.targaltinternetis.ee/en/about-the-project/ , 25 January 2019.

3. LEGAL FRAMEWORK

This chapter looks at Estonian legislation and finds how the laws regarding cyber violence are interpreted.

3.1. The Constitution and Civil Law

The Constitution of the Republic of Estonia (hereinafter as PS) declares fundamental rights in addition to freedoms towards people. Its provisions are implemented and operationalised in some cases of cyber violence that address dignity or freedom of privacy.

Defamation is an offence that can affect reputation and dignity. The Constitution §17 prohibits slandering one's honour or good name.[49] This right is important, because on one hand, image works as a self-esteem of a person who he is and on the other hand, it is how the person is shown to the public.[50] Hence, the protection of such fundamental right is needed since the public may form their opinions based on prejudice and they could be wrong like if someone disrespects the person by lying. Due to other fundamental rights given to the people in addition in the Constitution, it can be often questioned when the hate speech starts. Article 45 of the Constitution states the following: "Everyone has the right to freely disseminate ideas, opinions, beliefs and other information by word, print, picture or other means".[51] According to this right, people can more or less say whatever they feel like, but there are some restrictions. Commented edition of the Constitution explains that with such right obligations and liabilities still apply.[52] Article 45 also sets limitations by the law if the freedom of speech violates someone's honour, moralities and good name.[53] Law of Obligations Act (hereinafter as VÕS) has provisions that takes action in such cyber violence case. VÕS §1046 prohibits any kind of unlawful libel whether it is an inappropriate value judgement or a damage to one's private life and apart from that, VÕS §1047 does not allow defamatory information unless the owner declares its

[49] The Constitution of the Republic of Estonia. RT I, 15.05.2015, 2., p. 2.
[50] Maruste, R. (2017). *Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne.* §17, comm. 1. Accessible: https://pohiseadus.ee/index.php?sid=1&ptid=22&p=17 , 5 May 2019.
[51] The Constitution of the Republic of Estonia (2015), *supra nota* 49, p. 5.
[52] Maruste, R., Turk, K. (2017) *Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne.* §45, comm. 21. Accessible: http://www.pohiseadus.ee/index.php?sid=1&pt=&p=45#c21 , 5 May 2019.
[53] The Constitution of the Republic of Estonia (2015), *supra nota* 49, p. 5

rightness.[54] Therefore, defamation as cyber violence is protected under civil law, because the behaviour includes stating wrong information about potential victims like defined in the first chapter. They can claim for damages in the civil court since it is a civil matter.

Other cyber violence cases are criminalised under the criminal law, hence examined in the Penal Code chapter. However, the Constitution has fundamental rights that comply with the entitled freedoms for the victims of cyber violence regardless its types. For instance, PS §18 says that nobody can be tortured or treated degradingly.[55] This applies to cyberstalking, cyber harassment, outing and sextortion offences. People are often humiliated, threatened and left with mental as well as physical abuse in the aftermath. According to the commented edition, derogating treatment includes actions such as mocking, threatening, caused pain and other sufferings.[56] There is a court case about cyber harassment and cyberstalking in this chapter illustrating such behaviour.

Outing and catfishing are clearly criminal offences, but its victims are entitled to certain rights as well. PS §26 gives rights to private life without any interference unless it is necessary by the law.[57] This means that a person gets to choose if and to what extent his personal data is exposed.[58] For instance, when someone posts photos on Facebook, the owner has a right to adjusts its settings whether the post is seen by everybody or just among friends. A friend of the owner sees the photo and decides to use it without permission for whatever reason, thus there is a violation of the fundamental right. Apart from that, PS §43 protects the confidentiality of messages.[59] The commented edition of the Constitution defines the covered messages here as which the person only wants to share with some people.[60] With that being said, offenders of outing are breaking the fundamental right in addition to criminal law seen in the next subchapter, because the same element was in case of outing too. When courts make decisions on the given facts, they can mention which entitled right was breached among the applicable provisions from the Penal Code.

---

[54] Law of Obligations Act. RT I, 20.02.2019, 8., p. 273.
[55] The Constitution of the Republic of Estonia (2015), *supra nota* 49, p. 2.
[56] Maruste (2017), *supra nota* 50, §18, comm. 13. Accessible: http://www.pohiseadus.ee/index.php?sid=1&pt=&p=18#c13 , 5 May 2019
[57] The Constitution of the Republic of Estonia (2015), *supra nota* 49, p. 3.
[58] Jaanimägi, K., Oja, L. (2017) *Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne.* §26, comm. 24. Accessible: http://www.pohiseadus.ee/index.php?sid=1&pt=&p=26#c24 , 5 May
[59] The Constitution of the Republic of Estonia (2015), *supra nota* 49, p. 5.
[60] Laos, S., Sepp, H. (2017) *Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne.* §43, comm. 2. Accessible: http://www.pohiseadus.ee/index.php?sid=1&pt=&p=43#c2 , 5 May 2019

3.2. Penal Code

Estonian Penal Code (hereinafter as KarS) is considered as the main document when defining the criminal offences. Majority of cyber violence cases are criminalised.

Outing as a cyber violence falls under the provision of KarS §156, because it prohibits breaching the confidentiality of sent messages.[61] According to the commented edition of the Penal Code, a message is something that the sender only wants to share with certain people.[62] This already applies to the definition of outing stated in the first chapter. Accordingly, an offender criminalised under KarS §156 is a person neither of those who were meant to see the text.[63] The applicable scenario would be when someone sees a mailbox open on the computer with unread emails. He clicks on these to read and uses the information found for later publishing without the receiver's consent. This example is a clear violation of confidentiality. Another related provision to outing is KarS §157 prohibiting to publish personal data when done unlawfully.[64] Here it is important to mention that its validity is only in situations when the offender is in a professional activity due to what the data was received.[65] KarS §288 defines the professional as a person who is in entitled position for public tasks.[66] Therefore, when a worker shares information acquired from the duties such as professional secrecy, it is considered as a violation under KarS §157 in accordance with KarS §288 to prove the affiliation.

Moreover, Penal Code §157^2 prohibits unlawful use of someone's identity.[67] The provision has many elements that make it into criminal offence. For instance, sharing the information with third people, making the personal data available online and using it for other purposes.[68] There is no consent from the owner.[69] Identity theft known as catfishing falls into that scope, because it meets the requirements. Like previously declared, it means using someone's photos and data with no authorization. Due to this, intentional damage can be caused to the owner. KarS §157^2 also recognises intent as well as

[61] Penal Code. RT I, 13.03.2019, 77., p. 48.
[62] Sootak, J. Pikamäe, P. (2015). *Karistusseadustik. Kommenteeritud väljaanne*. Tallinn: AS Juura, p. 446.
[63] *Ibid*.
[64] Penal Code (2019), *supra nota* 61, p. 48.
[65] Sootak, J. Pikamäe, P. (2015), *supra nota* 62, p. 447
[66] Penal Code (2019), *supra nota* 61, p. 80.
[67] *Ibid.*, p. 48.
[68] Sootak, J. Pikamäe, P. (2015), *supra nota* 62, p. 450.
[69] *Ibid.*, p. 451.

damage to interests under the provision.[70] Thus, whoever is using stranger's images for fake profiles declaring that these belong to oneself, violates the owner's rights, and is committing an identity theft under Estonian Penal Code.

Cyberstalking and cyber harassment fall into the scope of KarS §157[3]. It prohibits continuous contact pursuit, stalking or other disturbance against the victim with an intent to cause threatening or humiliation.[71] Surveillance is only allowed if there is a legal right to do so, such as police investigation.[72] As seen in the definition chapter above, both acts of cyber violence have these elements. Offenders use threats of violence so the victim would feel insecure. In that case, KarS §120 is also applicable: "A threat to kill, cause health damage or cause significant damage to or destroy property, if there is reason to fear the realisation of such threat, is punishable by a pecuniary punishment or up to one year's imprisonment."[73] This provision contains many elements that relate to these two violations. Firstly, mental health is affected the most by threatening which includes either physical or material damage.[74] Threatening makes victims feel insecure and gives awareness like the loss promised is in the hands of the offender, because of the persuasion.[75] It does not matter whether they know each other or not, but the intent to terrorise is important – without purpose to cause fear it becomes invalid.[76] For instance, a cyber-stalker tells friends he is going to show up tomorrow and set the wife's car on fire. This is not valid as a threat, because the plan is known, friends are able to inform the potential victim. According to the commented edition, when the harasser really commits the crime he promised, then he is convicted of that particular offence under related provisions.[77] Another fictional example would be when a harasser threatens to kill the girl if she would not pay him 1000 euros. She feels terrified, but does not have such money and therefore gets murdered due to what he would receive a criminal offence in killing.

[70] *Ibid.*
[71] Penal Code (2019), *supra nota* 61, p. 49.
[72] *Ibid.*, p. 42. §137
[73] *Ibid.*, p. 38.
[74] Sootak, J. Pikamäe, P. (2015), *supra nota* 62, p. 381.
[75] *Ibid.*, p. 382.
[76] *Ibid.*, p. 382-383.
[77] *Ibid.*, p. 384.

Council of Europe in its report recognises revenge porn as a part of cyber violence. This term is for publishing and sharing sexual materials without the subject's authorisation as a revenge.[78] It can be also a serious violation towards children if they are involved which raises issues with child pornography. Overlapping activities are sextortion and sexting with slight differences, because all three involve sexual offences. Denmark has a case law concerning the issue of revenge porn. Minors were filmed during intercourse as they both agreed, but the girl was abused of which she did not give the consent to.[79] The footage was posted on Facebook and as it went viral, many people were able to watch as well as save it.[80] Danish police convicted over 1000 people of child pornography due to sharing since the couple was underage.[81]

Estonian criminal law also strongly prohibits child pornography. KarS §178 convicts anyone up to three years imprisonment who produces, publishes, shares or stores photos or videos in a pornographic as well as erotic situation of minors less than 14 years.[82] The provision includes elements that fall into the scope of revenge porn, sexting and sextortion. KarS §178 considers the material applicable if it shows someone under 18 as well as less than 14 years erotically where the understanding is enough.[83] The work is produced when it is recorded, accessible if made available for the public and showing such videos or photos.[84] Moreover, the material is considered to be stored when it is bought or rented.[85] Revenge porn meets the requirements, because its offenders are capturing sexual activities, keeping the work to use it and share online like in the Danish case. Same provision is applicable in sextortion as it overlaps with revenge porn. When sextortion or revenge porn is between adults, the behaviour can be penalised under KarS 157[1] – disclosure of special data.[86] Estonian legislation follows General Data Protection Regulation which defines such data in Article 9(1) where it is declared that data processing about someone's sex life is not allowed without authorisation.[87] Therefore, materials

[78] T-CY Mapping Study on Cyberviolence (2018), *supra nota* 4, p. 9-10.
[79] Sorensen, M. S. (2018). *1,000 Danes Accused of Child Pornography for Sharing Video of Teens.* Accessible: https://www.nytimes.com/2018/01/15/world/europe/denmark-child-pornography-video.html , 6 May 2019.
[80] *Ibid.*
[81] *Ibid.*
[82] Penal Code (2019), *supra nota* 61, p. 52.
[83] Sootak, J. Pikamäe, P. (2015), *supra nota* 62, p. 473.
[84] *Ibid.*
[85] *Ibid.*
[86] Penal Code (2019), *supra nota* 61, p. 48.
[87] European Parliament and the Council. Regulation 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). Brussels, OJ L 119, 4.5.2016.

illustrating adults in pornographic or erotic situations are protected. Offenders cannot share or publish it, unless the data is clearly made available by the person itself.[88] For instance, KarS 157[1] and GPDR Art. 9 (1) do not fall in the scope of sextortion or revenge porn when the offender took pornographic photo from the victim's social account – it has already been published.

Apart from that, when children send sexual text messages including such media between each other, it also follows the criteria for child pornography. In Cumberland two underaged teens were sexting and sending nude photos of themselves to each other due to what they faced felony charges after.[89] News added the youth is unconscious that sexting falls into the criteria of a child pornography under criminal law when it involves minors.[90] In addition to KarS §178, KarS §179 is also violated during sexting. It is prohibited to sexually tempt children by handing over the pornographic work or making it accessible as well as showing acts of sexual abuse and having sexual intercourse in front of them.[91] Tempting by KarS §179 includes talking about sexual topics, masturbating in front of a child or influencing them to become horny.[92] Thus, it can be assumed that when a child receives a text from the predator asking for a nude photo or talks about such topics, the criminal offence is committed.

Sextortion can raise issues with computer intrusions in addition, because like it was already explained in its related definitive chapter, offenders usually claim they have watched their potential victims through certain programs. Penal Code includes many provisions that regulate different infringements regards the process of sextortion. To be exact, KarS §206 prohibits disruption to computer data such as unlawful changes or deletion while KarS §213 prohibits computer frauds for gaining benefits and KarS §217 unlawful access to computers.[93] Due to that mentioned claim above, it can be assumed that offenders interference the systems by entering spyware or malware on the computers to watch its users through the activated web camera. In addition to such assumption, the spyware in turn can cause damages to the data which is already in the computer. Sextortion can be for benefits – offenders warn to publish the photos or videos of a potential victim unless money is given to them.[94] With the help of

[88] *Ibid*., p. 38. Article 9 (2)e.
[89] Blythe, A. (2015). *Consensual 'sexting' between Cumberland teens raises questions about criminal law.* Accessible: https://www.newsobserver.com/news/local/crime/article34971081.html , 6 May 2019.
[90] *Ibid.*
[91] Penal Code (2019), *supra nota* 61, p. 53.
[92] Sootak, J. Pikamäe, P. (2015), *supra nota* 62, p. 477.
[93] Penal Code (2019), *supra nota* 61, p. 60, 62, 64.
[94] T-CY Mapping Study on Cyberviolence (2018), *supra nota* 4, p. 11.

such malware to record people and access the computer data makes it an illegal act under KarS §213. Overall, KarS §216[1] prohibits the preparation of possible computer fraud which allows people to commit criminal offences under these computer-crimes.[95] This means that collecting data or making programs for the potential victims is also a violation.

Moreover, Estonian Penal Code §214 prohibits extortion which includes threats to expose humiliating data, cause damage or use violence.[96] This provision falls perfectly into the scope of sextortion, because it includes these elements required for blackmailing. To be a criminal offence, it does not matter whether the threat is fake or not – if the victim feels scared it is already valid.[97] Therefore, when someone receives a sextortion letter and considers this serious as well as scary, the offender is criminalised under the KarS §214 provision. However, when the recipient does not care and finds it as a joke, then the sender cannot be punished.

3.3. Findings

After being examined the Constitution and the Penal Code, some legal gaps were found.

At first, there is no clear interpretation regards cyberbullying. There are projects, campaigns as well as webpages on how to stay safe online, but the solutions need to go in depth with the laws. Without exact laws the government cannot control the spread of cyber violence nor cybercriminals. Thus, it is needed to have a legal recognition for privacy.[98] Cyberbullying is a serious online violation, because it can lead to suicides.[99] It might happen due to victims feeling unsupported and scared. The Constitution gives a fundamental right to no discrimination.[100] However, the right cannot do a lot if there is a gap between the law that could punish or act in case of cyberbullying. There would be no grounds for the court to arrest someone if the applicable provisions for the behaviour are missing.

[95] Penal Code (2019), *supra nota* 61, p. 63.
[96] *Ibid.*, p. 62.
[97] Sootak, J. Pikamäe, P. (2015), *supra nota* 62, p. 583.
[98] Marsoof, A. (2011). Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression. – *International Journal of Law and Information Technology*, Vol. 19, No 2, 110-132, p. 115.
[99] Rosen, L. D., Cheever, N., Carrier, L., M. (2015). *The Wiley Handbook of Psychology, Technology, and Society*. UK: John Wiley & Sons, p. 142.
[100] The Constitution of the Republic of Estonia (2015), *supra nota* 49, p. 2. §12.

Another legal gap in the regulatory framework addressing cyber violence is incitement to self-harm. The situation is the same: there are no exact laws to regulate such behaviour. It can be assumed when there are crimes that are committed during cyber violence, then the police can react in terms of law under those provisions that regulate such crimes. For example, if the victim is also kidnapped, the predator would fall and get penalised under the provisions that cover kidnapping. KarS §151 prohibits temptation to hate, but the provision says it is only valid when it is done publicly.[101] Therefore, it does not cover incitement of self-harm fully since it may be private too. The provision should be improved or clarified for the better online environment, because cyber violence can affect badly, like in the case of Blue Whale mentioned in this cyberbullying chapter.

For examining purposes, current consequences of some frauds were possible to be formed on assumptions from available rules. This leads to a conclusion that criminal proceedings towards cyber violence are limited. Victims cannot file criminal offences to all cyber violation cases no matter how serious it may be if there is a lack of legal grounds for criminalisation. Hence, some cyber violence cases can be solved by the civil court. This seems to tend more on the negative side, because every form of cyber violence is equally serious and important to deal with. Such behaviour might not be entirely controlled if there are still ways to commit them or laws that do not make offenders think before they take action.

In addition to legal framework, there are many blueprints covering bits of cyber violence regards other categories. Strategy for Violence Prevention 2015-2020 declares that by the year 2020 there are less assaults and victims receive aid.[102] Given steps to fulfil the goals are working with international recommendations, making therapies for criminals and training specialists who deal with the offences.[103] This could slightly help since constant work is in process. With the programs, they might be able to raise awareness about the current problem. For now, cyber violence seems like a new issue in the society, because of the scope that is covered. As to the therapies, it is declared that those who

[101] Penal Code (2019), *supra nota* 61, p. 46-47.
[102] *Vägivalla ennetamise strateegia aastateks 2015–2020*. Kriminaalpoliitika., p. 5. Accessible: https://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/vagivalla_ennetamise_strateegia_aastateks_2015-2020.pdf , 5 March 2019.
[103] *Ibid.*, p. 13-15.

get bullied on the web are usually getting it offline also.[104] This means the sessions with offenders would be mentally helpful for them. Considering the Strategy, the best result from there could be diminishing cyberbullying, cyberstalking or cyber harassment.

People in Estonia have faced sextortion as brought out in its related chapter above. It is a serious violation of dignity as well as the right to privacy. Law needs to strengthen sexual offences to control the situation even better. Image abuse is not bad only to the person it is sent, but also the culture is affected.[105] For example, people can lose jobs, difficult to find a new place for a living or they suffer mentally. In the latest Cyber Security Strategy 2019-2022 provided by Ministry of Economic Affairs and Communications, it is said that Estonia will manage to work with cyber threats and offer a secure digital society.[106]

3.4. Case law

The case study illustrates cyber harassment, cyber stalking and sexting. Mr. Kärdi is divorced from his ex-wife T. K. From July 2018 to August 2018, he called her countless times and even at night, strongly affecting TK.[107] She also received explicit messages in which the ex-husband humiliated her.[108] More discomfort was caused, because his behaviour was not limited to the phone. For instance, TK was followed and attacked when she left her house in addition to ex walking in her bedroom and throwing her against the wall, causing physical injuries.[109]

On these grounds, Mr. Kärdi was found guilty in many offences. These offences were qualified as criminal violations towards Estonian Penal Code. In general, he was sentenced 1 year 2 months and 13 days imprisonment, because the court merged all infringements and Mr. Kärdi was in a pre-trial

[104] Peebles, E. (2014). Cyberbullying: Hiding behind the screen. – *Paediatrics & Child Health*, Vol. 19, No. 10, 527-528, p. 527.
[105] McGlynn, C., Rackley, E. (2017). Image-Based Sexual Abuse. – *Oxford Journal of Legal Studies*, Vol. 37, No. 3, 534-561, p. 551.
[106] *Küberturvalisuse strateegia 2019-2022*. Majandus- ja Kommunikatsiooniministeerium, p. 4. Accessible: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf , 5 March 2019.
[107] PMKo 1-18-8865, p. 2-3.
[108] *Ibid.*, p. 3.
[109] *Ibid.*

detention.[110] Solely for harassment stalking he got six months in prison according to KarS §157^3 and four months due to threatening covered by KarS §120 (1).[111]

This case illustrates how the Penal Code provisions KarS §157^3 and KarS §120 work in practice. Mr. Kärdi constantly terrorised his ex-wife, such treatment usually causes problems with mental health in addition. She was humiliated, so during that time her life quality was also lowered. The ex's behaviour shows threats of violence which means she felt anxiety and was under constant terror. KarS §120 conditions for threats are fulfilled. As a reminder, it required for believable threats to the victim to receive a criminal offence under this provision.[112] Constant calls as well as contact search like following the victim, fall under the KarS §157^3 – performance of harassment.[113] Therefore, the court has provided its decision in accordance with the applicable law and should have done nothing differently.

[110] *Ibid.*, p. 4.
[111] *Ibid.*
[112] Sootak, J. Pikamäe, P. (2015), *supra nota* 62, p. 383.
[113] Penal Code (2019), *supra nota* 61, p. 49.

4. ESTONIA VS. EU COUNTRY

The Criminal Code of Finland and Spain are examined to draw a comparison between Estonian criminal law in accordance with these countries.

4.1. Finland

Finland has a Cyber Security Strategy helping to prevent cybercrimes and make online environment more secure. Although the main focus of such documents is always on state's preparedness against bigger crimes like cyberattacks, Finnish Strategy includes points which could also improve the scope of cyber violence among individuals. For instance, raising awareness between people who are dealing with the security, as well as in-depth examining by the police to solve facing problems.[114] Moreover, Finns have a separate document for society strategy planning creating risk analyses to get more control over the violations.[115] These two goals come in handy for the future since Finland does not have specific laws yet to cover fully each type of cyber violence. Nevertheless, some forms can be slightly covered by the Criminal Code of Finland (*Rikoslaki*).

Cyberstalking can be regulated by two provisions under Chapter 25 where one of them is Section 7(a) declaring that whoever is constantly stalking and creating distress receives a fine or a detention for up to two years.[116] Another rule sets consequences for coercion which is same as in case of stalking. Section 8 prohibits unlawful threatening caused to get what one desires.[117] Cyber harassment on the other hand, does not seem that serious due to the available penalty. The maximum punishment is only half a year in prison when constantly disturbing someone by calls or texts.[118] Therefore, this rule can be considered in case of sentencing a person for that cyber violence, because it matches with the previously found definition of cyber harassment.

---

[114] *Finnish National Cyber Security Strategy*. European Union Agency for Network and Information Security., p. 7-8, point 2 and 4. Accessible: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/finlands-cyber-security-strategy , 23 January 2019.
[115] *Security Strategy for Society.* Turvallisuuskomitea., p. 59. Accessible: https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf , 23 January 2019.
[116] Rikoslaki 19.12.1889/39., p. 115.
[117] *Ibid.*
[118] *Ibid.*, p. 108. Chapter 24, Section 1(a).

Finnish Criminal Code has also many provisions concerning sexual offences, but it is unclear whether these are enough for determining sexting-sextortion. For instance, it is prohibited to commit sexual abuses of a child including sexual services or sharing exposed images.[119] General rules come into account. The reason why it is unclear is that the provisions mention children, but like explained above, the act occurs among adults as well. Moreover, the Code under Chapter 20 Section 8(b) penalises anyone who is offering or tries to meet for sexual intentions.[120] The point can be slightly applicable towards cyberstalking, since the violation can include child abusers.

Outing as a type of cyber violence can occur easily, for example, opening someone's letter without permission. In the Criminal Code under Chapter 38 Section 3 the behaviour is named as "message interception".[121] Spreading false information is also considered a breach, hence for those actions, an offender can be penalised by imprisonment.[122] Looks like Finnish government is taking most cyber violence infringements seriously and cover as much as possible, so people could feel more secure while being online.

Apart from the forms of cyber violence examined above, catfishing as identity theft falls more or less under the Criminal Code of Finland. To be more exact, illegal access to computers and data collection stated in Chapter 38 Section 8, is a crime worth either a fine or detention.[123] It seems that fixed penalty depends on the facts, since catfishing is a wide term for taking over someone's identity. Lastly, any kind of extortion whether small or serious is a criminal offence covered by the Code.[124]

4.2. Spain

Spain has an extensive version of Criminal Code (*El Código Penal*) determining various criminal offences. Once again like with previous countries, some of the provisions fall slightly into the scope of cyber violence. These are observed in detail below.

[119] *Ibid.*, p. 86. Chapter 17, Section 18 and 18(a).
[120] *Ibid.*, p. 95.
[121] *Ibid.*, p. 154.
[122] *Ibid.*, p. 154, 110-111. Chapter 38 Section 3, Chapter 24, Section 9 and 10.
[123] *Ibid.*, p. 156-157.
[124] *Ibid.*, p. 132. Chapter 31, Section 3 and 4.

To begin with, Article 169 declares frightening treatment causing harm to the victim or other persons related by actions against freedom, privacy, morality and so forth.[125] This can be applicable in almost any type of cyber violence, because the overall goal of the behaviours is the same – to intimidate the victims.[126] Moreover, mental violence towards anyone which damages victim's integrity is punished with imprisonment according to the Article 173.[127] Cyber harassment as well as cyberbullying are assumingly covered by that article. Both of these actions include humiliating negative messages towards people affecting their mental health and lower self-esteem. If the abuse is sexual, then it is considered a criminal offence instantly.[128]

Sexual assault is a broad topic in the Criminal Code. For instance, one of the first provisions under the related chapters says: "whoever offends against the sexual freedom of another person, using violence or intimidation, shall be punished for sexual assault with a sentence of imprisonment from one to five years"[129]. By this provision, it can be said that sextortion messages are slightly covered since it involves offending sexual freedom. The criminal law also prohibits sexual abuse with children. In Spain, sexual intercourse or abuse with children who are younger than thirteen, are punished with up to six years in jail and if it is done by threatening, the sentence raises up to ten years.[130] It is worth to mention, because sexting-sextortion and cyberstalking can escalate fast into something physical. Moreover, cyberstalking as an attempt to meet for sexual purposes is covered by the Article 183 bis, because it prohibits the use of Internet or other communication methods to contact a minor with the purposes to meet up for such reasons.[131] Stalking in general is not allowed, but it turns into a bigger offence when children are affected and used for impropriate reasons like seen above.

Furthermore, sexting seems to be everyone's own preference for controlling as long as no one gets hurt. If sexting occurs and minors are involved then it is strongly forbidden under Article 189 that is prohibiting to show, share or make pornographic material.[132] This means people cannot demand for explicit images of youth and if such photos are sent, these must not be used. Extortion also falls into

[125] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal., p. 68.
[126] T-CY Mapping Study on Cyberviolence (2018), *supra nota* 4, p. 5.
[127] El Código Penal (1995), *supra nota* 125, p. 71.
[128] *Ibid.*, p. 76-77. Article 184.
[129] *Ibid.*, p. 74. Article 178.
[130] *Ibid.*, p. 75. Article 183 (1)-(2).
[131] *Ibid.*, p. 76.
[132] *Ibid.*, p. 78-80.

criminal offence declaring not to use force to get what desired.[133] This is like in the case of sextortion, because both actions are blackmailing. According to the Criminal Code Article 243 that related crime is punishable up to five years in prison.[134]

Other forms of cyber violence like outing, catfishing and related computer-crimes are also more or less covered by the law. For instance, identity theft as a part of catfishing is punished with detention of maximum three years and for data interference the penalty is the same.[135] Therefore, it shows that majority of cyber offenses are covered by the Code either way since digitalisation brings many online hazards. In the Cyber Security Strategy, they promise to improvement the legal framework further.[136] According to that, it can be assumed Spain may get improved regulations regards cyber violence.

4.3. Outcome

When it comes to Estonia vs. Finland, both countries are in a similar position. There are applicable provisions found under the criminal law, but the coverage of some provisions can be a bit unclear or complex. However, they do not differ drastically from each other. Cyber violence seems like a new problem to societies since they are now starting to focus on balancing the manners in cyberspace seriously.

As to the comparison of Estonia vs. Spain, there are more findings. The similarity is that both countries try to protect their citizens. However, it is seen Spanish Criminal Code is stricter with the laws. For instance, in Estonia a person who commits sexual crime towards a minor gets sentenced to imprisonment up to five years whilst in Spain, the punishment is up to six to 10 years.[137] This is one of the major factors showing Estonian laws are lenient when it comes to criminal offences. Another difference is the extensiveness of the Spanish Criminal Code – many details and cases are prohibited. Although the provisions are not exactly focused on cyber violence, consistency is found more or less.

[133] *Ibid.*, p. 93. Article 243.
[134] *Ibid.*
[135] *Ibid.*, p. 146, 100. Article 401, 264 (1), 264 bis (1).
[136] *Spanish National Cyber Security Strategy*. European Union Agency for Network and Information Security, p. 33, 35. Accessible: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/the-national-security-strategy , 23 January 2019.
[137] Penal Code (2019), *supra nota* 61, p. 45. §145 ; Código Penal (1995), *supra nota* 125, p. 75. Article 183 (1)-(2).

Spain has also updated their Cybersecurity Code this January observing the possibilities of a state and the actions for a better security, but it is not available in English language yet.[138]

National Cyber Security Strategies help creating ways how to tackle the problem with cybersecurity in general, so there are always some points affecting cyber violence. As previously mentioned, both three countries have their own strategies. Their main focus is on strengthening the system. It is good to know that Estonia, Finland and Spain are constantly working towards safer cyberspace with their own capabilities. Cyberspace is not the same with the regular, it needs other approach.[139]

[138] Código de Derecho de la Ciberseguridad.
[139] Kulesza, J. (2012). *International Internet Law.* USA: Routledge, p. xii.

5. RECOMMENDATIONS

Laws are keeping social order, so when something is missing or changed, the control needs to be renewed.[140] When it comes to cyber violence in Estonia, it is seen that Estonia has laws which need an improvement. The importance of national safety is not only because it protects individuals, but also helps the whole environment.[141] Author gives recommendation on how to find threshold of tolerable behaviour in accordance with the findings.

It is not easy to know the source or if someone has hacked the computer.[142] Therefore, cyber violence such as cyberstalking could easily occur. Due to anonymity, victims may not know who is harassing them.[143] One way how to balance the problem is strengthening the Penal Code as a whole. Spain has various types of cybercrimes covered in their national Criminal Code. Estonia should recognise more cyber violence forms in a clear manner. As of today, there are no exact provisions found in the Penal Code regards incitement to self-harm and cyberbullying. Thus, not much support from the law enforcement. These are all infringements that need action, because without it can become into chaos. Young people are more prone to the online risks due to their knowledge.[144] It means the state has to act quickly to get cyber violence under control, because children can be affected as well like seen from the child pornography perspective. Moreover, the consequences for criminal offences found in the Penal Code must become stricter. For instance, increasing the years of imprisonment. The applicable provisions of cyber violence are a bit weak – these would not make an offender think twice whether the breach is worth getting caught or not.

On that note, defamation should be criminalised. Victims of defamation can currently find support from the Constitution that gives them a fundamental right to good honour.[145] Law of Obligation Act

[140] Shariff, S. (2009). *Confronting Cyber-Bullying: What Schools Need to Know to Control Misconduct and Avoid Legal Consequences*. Cambridge, England: Cambridge University Press, p. 2.
[141] Bellaby, R. (2018). Going Dark: Anonymising Technology in Cyberspace. – *Ethics and Information Technology*, Vol. 20, No. 3, 189-204, p. 192.
[142] Goldsmith, J. (2013). How Cyber Changes the Laws of War. – *European Journal of International Law*, Vol. 24, No. 1, 129-138, p. 135.
[143] Jameson, S. (2008). Cyberharassment: Striking a Balance Between Free Speech and Privacy. – *Commlaw Conspectus*, Vol. 17, 231-266, p. 248.
[144] Chadwick, S. (2014). *Impacts of Cyberbullying, Building Social and Emotional Resilience in Schools*. Cham: Springer, p. 12.
[145] The Constitution of the Republic of Estonia (2015), *supra nota* 49, p. 2.

helps regards as prohibiting defamatory behaviour.[146] Since it is not criminalised, people might not want to bother with the offenders who slander them online. They can often be afraid as well to go through the process of suing when the penalties are in money. Offenders pay for damages and it could happen again, because it is not significant lesson. The author considers if defamation was a criminal offence, there would be less hate in social media, news reports included. People would think carefully first before saying whatever comes to them.

Estonia needs a specific document for guidance concerning solely cyber violence, because the issue is growing. The guide should clarify the types of cyber violence in addition to its requirements when the law is valid. Information whether it is a civil or criminal offence should be also provided, because it would be helpful for everyone who wants to make a complaint. For now, there are some forms that are considered as civil law cases. Penal Code is a good source for covering cyber violence, but it includes other criminal offences as well. Hence it is too extensive and could lead to confusion which provisions are applicable or to what extent. If there was a specific guidance material alongside with the applicable provisions and comments, it would be more user-friendly. The court could look them up faster than having to scroll down the entire Penal Code. Estonia should create the material with the web constables, cyber specialists and with the Ministry of Economic Affairs and Communications.

To improve the laws addressing cyber violence, the government needs overall enhancement. For instance, better and constant training of IT-specialists would be useful such as having specific programs. Cyber actions can be challenging.[147] Estonia needs in-depth cooperation with the police as the body who secures the country. Moreover, international agreements or partnerships can be made when writing the laws. Awareness of exact cyber act is vital, because it can consist of many things.[148]

Lastly, data protection is most likely to become affected by cyber violence as well. It asks a lot of notice like cybersecurity.[149] In addition to the specific guide, Estonia should secure the online

[146] Võlaõigusseadus (2019), *supra nota* 54, p. 273. §1046, §1047.
[147] Weissbrodt, D. (2013). Cyber-Conflict, Cyber-Crime, and Cyber-Espionage. – *Minnesota Journal of International Law*, Vol. 22, 347-387, p. 349.
[148] Tsagourias, N. (2012). Cyber Attacks, Self-Defence and the Problem of Attribution. – *Journal of Conflict and Security Law*, Vol. 17, No. 2, 229-244, p. 232.
[149] Kuner, C., Svantesson, D. J. B, Cate, F. H., Lynskey, O., Millard, C. (2017). The Rise of Cybersecurity and its Impact on Data Protection. – *International Data Privacy Law*, Vol. 7, No. 2, 73-75, p. 73.

communications by creating a highly guarded system from cyberattacks and cyber violence. No matter how big or small the flaw can be, being an e-country requires better protection for data interference. People who write digital codes affect online personalities.[150] Therefore, the risk of cyber violence is rising due to having e-residence, e-health and many other things digitalised. If Estonia had powerful protection systems together with specific laws, cyber violence would be less likely to occur.

[150] Crawford, S. P. (2004). Who's in Charge of Who I Am?: Identity and Law Online – *New York Law School Law Review*, Vol. 49, No. 1, 211-230, p. 215.

CONCLUSION

We are living in a digital age where almost everything is available online. People use different media platforms daily to share their thoughts and lifestyle. Estonia being an e-country is imposed to a greater risk of cyber violence. Internet provides a good environment for the infringements since devices are connected all the time. People need to be more careful when they are sharing sensitive data, because anyone could be affected. Council of Europe conducted a report on cyber violence in many countries where the laws were examined to see how different states handle the phenomena. Estonia was also listed in their report, but there was a lack of legal framework. Thus, the author of this thesis wanted to find out by herself how the law regulates cyber violence.

The aim of the thesis was to find legal gaps in Estonian laws regards cyber violence and provide suggestions for improvement. There were doubts it is a new problem for the society to cover major of it. Hypothesis was made with two questions to support the validity of the outcome. It was stated that the regulatory framework addressing cyber violence is fragmented and requires consolidation. First question asked what are the legal gaps found in legal regulation of cyber violence and second, how to improve the legal framework.

At first, different types of the assaults were defined to understand the big scope of the issue. Since cyber violence is board, only most known forms of such behaviour were observed. Afterward it was found that 90% of citizens are using Internet connection daily. Another survey showed that 40% of people have faced cyber violence. Estonia has lately dealt with sextortion messages, so the problem is active and growing. Legal framework was examined and a case law followed to illustrate how Estonian court handled a cyber violence offence. It was also stated if the court should have done something differently.

Hypothesis turned out to be correct, because the author found many shortages. Penal Code is a lengthy document that regulates slightly some types of cyber violence. However, the applicable provisions are limited due to not being specific or clear enough in all cases. There are offences which needed further consideration to make sure of the relevance. This can lead to confusion, especially for an average reader who is not so familiar with the legal language. Moreover, there are types that do not fall into

the scope of criminal offence. Cyber violence that falls under civil matters is regulated by another documents. Therefore, the laws are too fragmented and not in one place. Cyberbullying and incitement to self-harm are not regulated, there is a major gap. Comparison was made between Estonia vs. Finland vs. Spain to see the differences as well as similarities. The author found that all states have strategies for national cyber security, but also miss some laws regulating the issue towards online cruelty. However, Spain is more convenient and has stricter penalties. It does seem that monarchy as a state power influences the laws in a strong way.

Therefore, first question can be answered as follows: Estonia has the Penal Code as a main document for criminal offences including provisions that are more or less applicable in certain cases of cyber violence. The document needs an improvement, because such provisions are not as clear as they should be like explained above. In addition, penalties are too lenient for serious offences. There is a lack of specific guidance material focusing on cyber violence. Most relevant laws are currently a bit too weak to provide a more secure cyberspace. Cyberbullying is not regulated by the criminal law. Defamation was found to be under civil law, but it should be considered as criminal offence, because every cyber violence is serious. Victims can receive remedies, but they could still be on the target – nothing stops the offenders behaving so if the laws are lenient or missing.

The answer to the second question is: Estonia needs to strengthen the laws, especially the Penal Code about requirements when the offence falls under those related provisions. In addition, the penalties should become stricter so it would make the offender think twice whether it is worth to get caught. There should be a guidance material dedicated only to cyber violence. It can define different types of online assaults, determine the penalties and whether it is a criminal or civil matter, so people would know the right court for settlement. Like explained in the first answer, defamation should be criminalised, because it is as serious as any other infringement. In addition, it is needed to create a system with a high level of supervision from cyberattacks and cyber violence. To do all what the author suggests, cooperation with the police, cyber specialists and Ministry of Economic Affairs and Communications is essential. International agreements are useful, but IT-specialists require constant training since technologies evolve rapidly. With a strong legislation it could be possible to reduce the amount of cyber violence.

For further research purposes, the author recommends extending the topic by examining the affect the EU General Data Protection Regulation has on Estonia and its laws. The focus can be on cyber violence in addition to cybersecurity. It could be determined whether the GDPR has helped to control the data interference and whether cyberattacks are less likely to occur due to the new regulation.

LIST OF REFERENCES

Science books:

1. Bauman, S. (2014). *Cyberbullying: What Counselors Need to Know.* USA: John Wiley & Sons.

2. Betts, L. (2016). *Cyberbullying: Approaches, Consequences and Interventions.* London: Palgrave Macmillan Limited.

3. Chadwick, S. (2014). *Impacts of Cyberbullying, Building Social and Emotional Resilience in Schools*. Cham: Springer.

4. Kowalski, R. M, Limber, S. P., Agatston, P. W. (2012). *Cyberbullying: Bullying in the Digital Age.* 2nd. ed. USA: Wiley-Blackwell.

5. Kulesza, J. (2012). *International Internet Law.* USA: Routledge.

6. Madise, Ü. *et al.* (2017). *Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne*. Tallinn: AS Juura.

7. Reuvid, J. (2010). *Managing Business Risk: A Practical Guide to Protecting Your Business*. 7th. ed. UK: Kogan Page.

8. Rosen, L. D., Cheever, N., Carrier, L., M. (2015). *The Wiley Handbook of Psychology, Technology, and Society*. UK: John Wiley & Sons.

9. Savin, A. (2013). *EU Internet Law.* Cheltenham, Gloucestershire: Edward Elgar Publishing Inc.

10. Shariff, S. (2009). *Confronting Cyber-Bullying: What Schools Need to Know to Control Misconduct and Avoid Legal Consequences*. Cambridge, England: Cambridge University Press.

11. Singer, P. W., Friedman, A. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press.

12. Sootak, J. Pikamäe, P. (2015). *Karistusseadustik. Kommenteeritud väljaanne.* Tallinn: AS Juura.

13. Subrahmanyam, K., Šmahel, D. (2010). *Digital Youth: The Role of Media in Digital Development.* New York: Springer.

14. Wall, D. (2001). *Crime and the Internet*. England: Routledge.

Peer-reviewed articles:

15. Al-Alosi, H. (2017). Cyber-violence: Digital Abuse in the Context of Domestic Violence. – *University of New South Wales Law Journal*, Vol. 40, No. 4, 1573-1603.

16. Bellaby, R. (2018). Going Dark: Anonymising Technology in Cyberspace. – *Ethics and Information Technology*, Vol. 20, No. 3, 189-204.

17. Crawford, S. P. (2004). Who's in Charge of Who I Am?: Identity and Law Online – *New York Law School Law Review*, Vol. 49, No. 1, 211-230.

18. Gillespie, A. A. (2013). Adolescents, Sexting and Human Rights. – *Human Rights Law Review,* Vol. 13, No. 4, 623-643.

19. Goldsmith, J. (2013). How Cyber Changes the Laws of War. – *European Journal of International Law*, Vol. 24, No. 1, 129-138.

20. Kuner, C., Svantesson, D. J. B, Cate, F. H., Lynskey, O., Millard, C. (2017). The Rise of Cybersecurity and its Impact on Data Protection. – *International Data Privacy Law*, Vol. 7, No. 2, 73-75.

21. Marcum, C. D., Higgins, G. E., Ricketts, M. L. (2014). Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration – *International Journal of Cyber Criminology*, Vol 8, No. 1, 47-56.

22. Marsoof, A. (2011). Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression. – *International Journal of Law and Information Technology*, Vol. 19, No 2, 110-132.

23. McGlynn, C., Rackley, E. (2017). Image-Based Sexual Abuse. – *Oxford Journal of Legal Studies*, Vol. 37, No. 3, 534-561.

24. McGlynn, C., Rackley, E., Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse – *Feminist Legal Studies*, Vol. 25, No. 1, 25-46.

25. Peebles, E. (2014). Cyberbullying: Hiding Behind the Screen. – *Paediatrics & Child Health*, Vol. 19, No. 10, 527-528.

26. Peterson, J., Densley, J. (2017). Cyber Violence: What Do We Know and Where Do We Go from Here? – *Aggression and Violent Behavior,* Vol. 34, 193-200.

27. Slaninova, G., Haviger, J., Novotna, L., Sochorova, P., Vackova, M. (2011). Relationship between cyberbullying and readiness for aggressive behavior in middle adolescence – *Procedia – Social and Behavioral Sciences*, Vol. 29, 567-573.

28. Svantesson, D. J. B. (2011). "Sexting" and the Law – 15 Minutes of Fame, and a Lifetime of Shame – *Masaryk University Journal of Law and Technology*, Vol. 5, No. 2, 289-303.

29. Tsagourias, N. (2012). Cyber Attacks, Self-Defence and the Problem of Attribution. – *Journal of Conflict and Security Law*, Vol. 17, No. 2, 229-244, 232.

30. van Laer, T. (2014). The Means to Justify the End: Combating Cyber Harassment in Social Media. – *Journal of Business Ethics*, Vol. 123, No. 1, 85-98.

31. Wall, D. S. (2005). The Internet as a Conduit for Criminals. – *Information Technology and the Criminal Justice System.* (Ed.) Pattavina, A. Thousand Oaks, CA: Sage Publications, 77-98.

32. Weissbrodt, D. (2013). Cyber-Conflict, Cyber-Crime, and Cyber-Espionage. – *Minnesota Journal of International Law*, Vol. 22, 347-387.

Estonian legislation:

33. The Constitution of the Republic of Estonia. RT I, 15.05.2015, 2.

34. Penal Code. RT I, 13.03.2019, 77.

35. Law of Obligations Act. RT I, 20.02.2019, 8.

Other countries' legislation:

36. Código de Derecho de la Ciberseguridad.

37. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

38. Rikoslaki 19.12.1889/39.

European Union legislation:

39. European Parliament and the Council. Regulation 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). Brussels, OJ L 119, 4.5.2016.

Court cases:

40. PMKo 1-18-8865.

Web materials:

41. *About the Project.* Targalt Internetis. Accessible: https://www.targaltinternetis.ee/en/about-the-project/ , 25 January 2019.

42. Arfi, N., Agarwal, S. (2013). *Knowledge of Cybercrime among Elderly*. Accessible: https://www.researchgate.net/publication/242654499_Knowledge_of_Cybercrime_among_Elderly , 25 January 2019.

43. Blythe, A. (2015). *Consensual 'sexting' between Cumberland teens raises questions about criminal law.* Accessible: https://www.newsobserver.com/news/local/crime/article34971081.html , 6 May 2019.

44. *Bullying.* Council of Europe. Accessible: https://www.coe.int/en/web/children/bullying , 23 January 2019.

45. *Catfish: The TV Show. About the Show.* MTV UK. Accessible: http://www.mtv.co.uk/catfish-the-tv-show , 24 January 2019.

46. *Catfishing.* The Cybersmile Foundation. Accessible: https://www.cybersmile.org/what-we-do/advice-help/catfishing , 24 January 2019.

47. *Cyber violence is a growing threat, especially for women and girls*. EIGE. Accessible: https://eige.europa.eu/news/cyber-violence-growing-threat-especially-women-and-girls , 7 May 2019.

48. *Finnish National Cyber Security Strategy.* European Union Agency for Network and Information Security. Accessible: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/finlands-cyber-security-strategy/ , 23 January 2019.

49. *Harassment and cyberbullying policy*. YouTube. Accessible: https://support.google.com/youtube/answer/2802268?hl=en , 23 January 2019.

50. *How Do I Report a Child Under the Age of 13?* Facebook Help Center. Accessible: https://www.facebook.com/help/157793540954833 , 23 April 2019.

51. *Küberturvalisuse strateegia 2019-2022*. Majandus- ja Kommunikatsiooniministeerium. Accessible: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf , 5 March 2019.

52. Mandri, J-M. (2018). *Järjekordne laine petukirjasid: RIA hoiatab sextortion-väljapressijate eest.* Accessible: http://forte.delfi.ee/news/digi/jarjekordne-laine-petukirjasid-ria-hoiatab-sextortion-valjapressijate-eest?id=83877899 , 24 January 2019.

53. *Minister Mailis Reps: küberkiusamise ennetamine on turvalise koolitee osa.* Haridus- ja Teadusministeerium. Accessible: https://www.hm.ee/et/uudised/minister-mailis-reps-kuberkiusamise-ennetamine-turvalise-koolitee-osa , 25 January 2019.

54. Pealinn. (2016). *LIGI 3000 KIUSAMISJUHTU: Küberkiusamine on Eestis terav probleem, ütlevad veebikonstaablid*. Accessible: http://www.pealinn.ee/koik-uudised/ligi-3000-kiusamisjuhtu-kuberkiusamine-on-eestis-terav-probleem-n163144 , 25 January 2019.

55. Rossow, A. (2018). *Cyberbullying Taken to a Whole New Level: Enter the 'Blue Whale Challenge'.* Accessible: https://www.forbes.com/sites/andrewrossow/2018/02/28/cyberbullying-taken-to-a-whole-new-level-enter-the-blue-whale-challenge/#177f02d82673 , 23 January 2019.

56. *Security Strategy for Society.* Turvallisuuskomitea. Accessible: https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf , 23 January 2019.

57. Sorensen, M. S. (2018). *1,000 Danes Accused of Child Pornography for Sharing Video of Teens.* Accessible: https://www.nytimes.com/2018/01/15/world/europe/denmark-child-pornography-video.html , 6 May 2019.

58. *Spanish National Cyber Security Strategy.* European Union Agency for Network and Information Security. Accessible: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/the-national-security-strategy , 23 January 2019.

59. Statistics Estonia. (2018). Quarterly Bulletin of Statistics Estonia. An overview of social and economic developments in Estonia 2/2018. – [E-database] https://www.stat.ee/publication-2018_quarterly-bulletin-of-statistics-estonia-2-18 (10 October 2018).

60. Tiitsmaa, S. (2017) *Noored IT-seadmete ja interneti maailmas.* Accessible: https://blog.stat.ee/2017/10/26/noored-it-seadmete-ja-interneti-maailmas/?highlight=internet , 25 January 2019.

61. *Vägivalla ennetamise strateegia aastateks 2015–2020*. Kriminaalpoliitika. Accessible: https://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/vagivalla_ennetamise_strateegia_aastateks_2015-2020.pdf , 5 March 2019.

Other materials:

62. Dempsey, J. S. (2010). *Introduction to Private Security*. 2nd ed. USA: Cengage Learning Inc.

63. Hickey, E. W. (2013). *Serial Murderers and their Victims*. 6th ed. USA: Cengage Learning Inc.

64. Jameson, S. (2008). Cyberharassment: Striking a Balance Between Free Speech and Privacy. – *Commlaw Conspectus*, Vol. 17, 231-266.

65. Kalmus, V. (2011). Ülevaade EU Kids Online Uuringu tulemustest. – *Turvalisuse interneti päeva konverents,* 11 February 2011 Tallinn. Tartu: University of Tartu.

66. Sciandra, M. (2017). *Cybercrime: Using Computers as Weapons*. USA: Greenhaven Publishing.

67. Sukk, M., Soo, K. (2018). Preliminary findings of the EU Kids Online 2018 Estonian survey: Summary. – *EU Kids Online Estonia*. (Eds). Kalmus, V., Kurvits, R., Siibak, A. Tartu: University of Tartu, Institute of Social Studies, 1-8.

68. T-CY Mapping Study on Cyberviolence 2018.