



FACULTY OF LAW
Lund University

Ekaterina Markovich

Two Clicks Away

An analysis of the offence of viewing child sexual abuse
materials on the Internet

JAMM07 Master Thesis

International Human Rights Law
30 higher education credits

Supervisor: Karol Nowak

Term: Spring 2017

Table of Contents

Preface	3
Summary	4
Abbreviations	5
1 Chapter One: Introduction	7
1.1 Background	7
1.2 Historical overview, Swedish example	9
1.3 The Aim and Research Questions	11
1.4 Terminology	12
1.5 Methodology and Theory	13
1.5.1 <i>Method and Materials</i>	13
1.5.2 <i>Theory</i>	14
1.6 Delimitations	17
2. Chapter Two: Viewing Child Sexual Abuse Materials on the Internet as a Criminal Offence	21
2.1 Defining Child Sexual Abuse Materials	21
2.2 Reflection of the Offences Related to Child Sexual Abuse Materials in International Legal Instruments	23
2.3 Child Sexual Abuse materials on the Internet: Accessibility, Availability, Assortment	25
2.4 Imitation, Stimulation or Inspiration: Relations Between Child Pornography and Child Sexual Abuse	28
2.4.1 <i>Models on Relationship Between Pornography and Sexual Crimes</i>	28
2.4.2 <i>From Viewing to Abusing</i>	29
2.4.3 <i>Psychological factors linking offences of child sexual abuse</i>	30
2.5 No Victim, No Harm, No Guilt	32
2.6 Criminalisation of Viewing: Harm Principle and Mens Rea	34
2.6.1 <i>Consequences of viewing child sexual abuse materials for children</i>	34
2.6.2 <i>Harm Principle</i>	35
2.6.3 <i>Mens rea: Deliberate Search For Child Sexual Abuse Materials and the Element of Knowing</i>	37
3 Chapter Three: Viewing Child Sexual Abuse Materials on the Internet as a Global Problem	40
3.1 Child Sexual Abuse Materials on the Internet: Globalisation and Collective Efforts	40
3.2 The Complexity and Complications of the Dark Web	43
3.2.1 <i>What is the Dark Web</i>	43
3.2.2 <i>Possibilities and Potentials to Control the Dark Web</i>	44
3.3 Fears and Concerns In Regards to Investigations on the Internet	46
3.4 Limitations Posed by Right to Private Life and Freedom of Expression	49
3.4.1 <i>Right to Private Life and Freedom of Expression</i>	49
3.4.2 <i>The US example</i>	50

3.4.3 <i>The EU approach on data protection</i>	51
3.4.4 <i>The ECtHR approach</i>	52
3.5 Jurisdictional Disputes and International Cooperation	55
3.5.1 <i>Jurisdiction</i>	55
3.5.2 <i>Cooperation</i>	56
4 Chapter Four: Combating Viewing Child Sexual Abuse Materials on the Internet	59
4.1 Call For Action	59
4.2 Obligations to Criminalise Viewing Child Sexual Abuse and Exploitation Materials on the Internet	61
4.3 A Need For a New Treaty v. the Use of Existing Instruments	64
4.3.1 <i>A New Instrument</i>	64
4.3.2 <i>The sufficiency of existing legislation</i>	65
4.4 Legal Regulation of the work of ISPs	68
4.5 The Potential of Corporate Social Responsibility in Combating the Offence of Viewing Child Sexual Abuse Materials on the Internet	72
4.6 Awareness and Advocacy: Role of Civil Society and NGOs	76
Concluding Remarks	80
Bibliography	83
Table of Cases	92

Preface

The research of this topic provided me with a deep knowledge and changed my perspective on crimes against children committed with the use of technology. Most of discoveries were far from pleasant, some were even disturbing. Thus, I believe it is important to warn a reader of this paper. The topic of this thesis, quotations and statistics might be upsetting, and I do understand reluctance to read on such an unsettling issue. Still, there is one thing I want a reader to remember. A hidden world of child sexual abuse materials is not as hidden as one would imagine and is much closer than we used to think. It is literally two clicks away if one knows where to look. It exists in much more diverse forms than it is commonly believed and it abuses and dehumanises real children in worst ways possible as long as materials are available on the Internet. That is due to the issue not being taken seriously in the international community. It also gives me a reason to carry out this research and continue with it from now on.

This thesis would not be possible without the scholarship granted to me by Svenska Institutet. I am thankful for the SI for giving me the opportunity to be a part of this master's programme, explore the new country and enjoy the unique study environment of Lund University and Raoul Wallenberg Institute of Human Rights and Humanitarian law. And thank you, Markus Boman and Madeleine Mattsson, for being here for me and for all of us during these two years.

I want to express my gratitude to my supervisor, Karol Nowak for his constructive comments on my paper, help in shaping my thesis structure and advices on defining my research topic. Thank you for your assistance and encouragement, and thank you for always answering my questions!

I would like to thank all the teachers working on the programme for inspiration, sharing your knowledge, support and understanding. I have learned a lot during this two years, and grew significantly as a lawyer, as a researcher, and as a person.

I want further thank honorable members of Capulus Clava for support, advices, all of the refreshing discussions on law beyond all borders, prohibition of thesis talk, and tremendous amounts of coffee. You are the best study circle one could wish for, you are amazing friends, and you will always have a special place in my heart. Special thanks for Léa Bozzi for being a wonderful group member and friend for every course we had together.

Last but not least, I am extremely grateful for my family, especially for my partner, Olga, for always believing in me, for your unconditional love and support that kept me going even during the darkest times.

Ekaterina Markovich,
24 May 2017,
Lund, Sweden

Summary

The core focus of the thesis is the phenomenon of viewing child sexual abuse materials on the Internet as a grave violation of human rights. The thesis is aimed to argue the criminal nature of the act of viewing child sexual abuse materials on the Internet, provide a brief analysis of its causes and effects, examine a legislative gap in protection of children's rights, and eventually seek to address potential solutions as the action must be taken and legislative gap must be closed on both domestic and international levels.

The problem of viewing child sexual abuse materials on the Internet had long gone unnoticed and been considered harmless and victimless. This attitude started to change over past decades but not much as one can see from the statistics. Thus the study made by Aftonbladet and Svenska Dagbladet shows that about 15 000 people from Sweden downloaded child pornography in 2016, but only 119 faced actual prosecution and just 20 were sent to prison in 2015. Statistics on viewers gathered by UK scientists demonstrate that more than 168 000 requests are made per day to the websites containing child sexual abuse materials. That illustrates that the existing legal protection of children's rights is not sufficient enough in relation to phenomenon of viewing child sexual abuse materials on the Internet.

An effective protection certainly demands collective efforts from the states, the need for which has been highlighted many times in the recent decades and reflected in case-law. Some efforts have been made to address the problem, however, they mostly concentrate on active participators. Yet, seldom the viewers of such content end up facing charges. That allows paedophiles to escape prosecution for watching children being sexually abused, simultaneously creating a demand for such production. The effects of this offence on children had been examined over the past decades clearly illustrating the vast negative impact the offence has over the child's development, dignity and rights. Yet, the notion of considering the crime victimless and harmless remains as viewing of child sexual abuse materials is not criminalised in many countries. That position, however, can no longer be legitimate in a modern world. There is always a victim behind every image, a child, whose human rights, health and dignity are being severely violated. A victim, that is re-victimised and dehumanised every time the material is viewed.

Abbreviations

ACHR - American Convention on Human Rights

AU - African Union

Budapest Convention/Convention on Cybercrime - Council of Europe Convention on Cybercrime

CJEU - Court of Justice of the European Union

CoE - Council of Europe

COP - Child Online Protection

CRC - UN Convention on the Rights of the Child

CSR - Corporate Social Responsibility

CtRC - Committee on the Rights of the Child

Data Retention Directive - Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Directive 2011/93 - Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

ECHR - European Convention on Human Rights

ECtHR - European Court on Human Rights

ECPAT - End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes

EU - European Union

EUROPOL - European Law Enforcement Agency

FBI - Federal Bureau of Investigation (US)

Global Alliance - Global Alliance Against Child Sexual Abuse Online

ICCPR - International Covenant on Civil and Political Rights

ICESCR - International Covenant on Economic, Social and Cultural Rights

ICMEC - International Centre for Missing & Exploited Children

ICT - Information Communication Technologies

ICSE database - International Child Sexual Exploitation database

ILO - International Labour Organisation

INHOPE - International Association of Internet Hotlines

INTERPOL - International Criminal Police Organisation

IP - Internet Protocol

ISP - Internet Service Provider

IT - Information Technology

IWF - Internet Watch Foundation

Lanzarote Convention - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

NCMEC - National Centre for Missing & Exploited Children

NGO - Non-Governmental Organisation

NIT - Network Investigative Technique

OAU - Organisation of African Unity

Ruggie Principles - UN Guiding Principles on Business and Human Rights

OPSC - Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

Tor - The Onion Router

UDHR - Universal Declaration of Human Rights

UN - United Nations

UNICEF - The United Nations Children's Fund

URL - Uniform Resource Locator

VPN - Virtual Private Networks

1 Chapter One: Introduction

1.1 Background

“Can you guys share the links to the clips where two men rape a school kid, and the kid is in pain, crying all the time, so it’s not gonna be, you know, the ‘pretend rape’?”

Anonymous

I found this post in an anonymous thread on one of the Russian forum services a few months ago, and it is a splitting image of what people who view child sexual abuse materials are looking for. The Internet provides billions of opportunities to fulfil such desires. Thus, the Internet Watch Foundation (IWF) in the United Kingdom reported that, out of all reports of child pornography received by IWF in 2014, 43% of images showed sexual activity between adults and children including rape or sexual torture.¹

Since the beginning of public use of the Internet, the spread of child sexual abuse materials among paedophile networks has grown remarkably. Viewing, sharing and collecting it became inexpensive, fast, low-risk and anonymous², so easy, that the crime has long been misinterpreted as “victimless”³, often with the emphasis of the absence of the harm element in viewing the content without storing or further distributing it. That, however, is a false impression which leads to dehumanisation of a real children abused and exploited for the purposes of producing such materials. It is important to keep in mind that behind each piece of material there is a real child being exposed to severe violations of his or her human rights. Moreover, with the nature of the Internet it presents to be nearly impossible to erase all the copies of the material after it has been published. The horrible evidences of child sexual abuse

¹ Internet Watch Foundation, Annual Report 2014, available at: <https://www.iwf.org.uk/sites/default/files/reports/2016-02/IWF%202014%20Annual%20Report%20%28web%29.pdf> (last visited 20 May 2017).

² Donna M. Hughes “The internet and sex industries: partners in global sexual exploitation” (2000).

³ “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016), available at: <http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf> (last visited 20 May 2017).

can stay online forever, showing the abuse over and over again for the pleasure of paedophiles from all over the world as there are no borders on the Internet. Meanwhile children grow up knowing that there are images or videos of them circulating over the Internet, which leads to anxiety, fears and other damages to child development.

The central claim of this thesis is therefore that viewing child sexual abuse materials is a crime, which must be incorporated in national legislation and combated both on national and international levels by joint efforts of law enforcement agencies, Internet service providers (ISPs)⁴ and IT companies.

⁴ For the purposes of this thesis any organisation that provides services to access and use the Internet would be considered as ISP.

1.2 Historical overview, Swedish example

Phenomenon of viewing child sexual abuse materials is not a new one, though it became the topic of public discussion only a few decades ago. The same can be said about the ideas on its alleged harmlessness for the real children “as it is only pictures”. As Sweden is one of the central countries used for my analysis, I will use its example to illustrate that pattern.

In 1992 the first child pornography raid occurred in Huddinge, leading to discovery of two men who produced the material with the participation of Swedish citizens, and sent it a lists of paedophiles within and outside the state via mail. A year later a new operation in Norrköping led to discovery of yet another paedophile network in Sweden. These two cases got a large attention from the media. It was possible to identify nine Swedish children associated with both operations. By mutual agreement between the police and the child and adolescent clinic at the University Hospital in Linköping, children's reactions and memories of abuse and later development had been closely monitored.⁵ The book on study results had been published by Save the Children Sweden in 1996, only a few month prior the first case of the Internet-based international paedophile ring called the “Orchid Club”⁶ had been uncovered. Materials obtained during Orchid Club investigation led to discovery of yet another paedophile network, the “Wonderland Club”⁷, prosecuted in 1998. To obtain membership in this organisation an individual was obliged to provide 10,000 unique pictures of children in different stages of sexual abuse. These shocking discoveries provoked a strong reaction from the public and lead to rather active discussions.

The problem of child sexual abuse remains of a large concern for the international community up until the present day. As a result, new numbers were presented for the public in Sweden by a joint study performed by two Swedish newspapers Aftonbladet and Svenska Dagbladet in 2016. The study showed that of over 14 857 people who downloaded child pornography in

⁵ C.G.Svedin, K. Back “Children who don’t speak out. About children being used in child pornogprahy”, Rädta Barnen Sweden (1996), p. 28.

⁶ One of the first prosecuted cases in which pictures of a child being molested were transmitted in a real time video conference with 11 people from different countries were sending the requests for the perpetrators via chat function, asking for various poses and abuses.

⁷ See for example, media reports on the case, BBC News (2001). Wickedness of Wonderland, available at: http://news.bbc.co.uk/2/hi/uk_news/1167879.stm (last visited 28 April 2017).

2016, and only 119 faced actual prosecution with just 20 were sentenced to imprisonment in 2015.⁸ Statistics on viewing (or accessing the materials) comes in numbers which are even larger.⁹ The discussion on the seriousness of the crime of child pornography is ongoing in a Swedish society. It is still unclear, however, what the future will bring. With the globalisation trend one can assume that the situation is not much different in other countries.

⁸ Aftonbladet, “15 000 laddade ned – bara 119 dömdes” (2017). The study is available (in Swedish): <http://anvandarna.story.aftonbladet.se/chapter/15-000-laddade-ned-bara-119-domdes/> (last visited 15 May 2017).

⁹ See, for example, G. Owen, N. Savage “The Tor Dark Net” (2015), Centre for International Governance Innovation and the Royal Institute of International Affairs, available at: https://www.ourinternet.org/sites/default/files/publications/no20_0.pdf (last visited 05 May 2017).

1.3 The Aim and Research Questions

The objective of this thesis is to examine a legislation gap on the protection of children against sexual abuse, more precisely against viewers of child sexual abuse and exploitation materials on the Internet. The thesis is also seeking to close the gap by addressing different aspects of the problem, such as its global nature, a technological impact of a high level, and need for harmonisation of national legislations and more coordinated collaboration on international level. The research questions of this thesis are the following:

- Whether viewing of child sexual abuse materials on the Internet is a criminal offence?
- How children's rights are protected against such offence by existing positive law, and what gaps can be identified in existing legal instruments?
- Which difficulties arise from the use of technologies and global nature of the offence?
- How these gaps and difficulties can be addressed from the perspectives of national legislation, regional and global instruments?
- What role do service providers, IT companies and civil society have in relation to combating the offence of viewing child sexual abuse materials on the Internet?

1.4 Terminology

This thesis presumes that the reader possess the basic knowledge of international law, thus widely known concepts would not be explained during the course of the paper. The nature of offence addressed in the current thesis calls for use of information communication technology (ICT) terminology. Most of the terms are explored in the context of the chapters aimed to address the technological side of the problem. Yet the basic knowledge of terminology is presupposed.

The term “*child*” is used for describing every human being below the age of eighteen years old.

The use of terms “*child sexual abuse*” and “*child sexual exploitation*” is advised instead of “*child pornography*” by ECPAT International in “Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse” adopted by the Interagency Working Group in Luxembourg, 28 January 2016. Still, the child pornography is more known, and many international and national legal instruments refer to it. Same goes for “*indecent images of children*” used in the UK. All these terms describe the same offence of documented abuse of children, their humiliation to the point of dehumanisation. Therefore it would be of importance to keep in mind that, the main focus of this thesis is the offence itself, not the terminology used to describe the offence.

1.5 Methodology and Theory

1.5.1 Method and Materials

During the course of analysis the dogmatic legal method is used to describe, examine and interpret legislation to pinpoint trends and gaps in it. An analysis of *de lege lata* provides the author and the reader with the status of legal protection of the children's rights against viewing child sexual abuse materials on the Internet. In order to fulfil the aim of this thesis, one should start by analysing the existing legislation. Thus, I ground it on the Convention on the Rights of the Child (CRC), Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography (OPSC). Regional legal instruments such as European Convention on Human Rights (ECHR), Council of Europe Convention on Cybercrime (Budapest Convention), and Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) are also examined alongside with supranational instruments, for example, EU Directives. A study of jurisprudence is also used in regard with the dogmatic legal method. Thus, I am addressing the case-law of the European Court of Human Rights (ECtHR), the Court of Justice of the European Union (CJEU), and national practices. The research also includes an analysis of existing legal framework on national levels (Sweden, the UK, Russia, the US, Canada)¹⁰. During the course of the thesis works of Gillespie, Buck, Van Bueren, Martellozzo, Akdeniz, Eneman, and Haasz in regard to children's rights, child sexual abuse and child sexual abuse materials, as well as law and technology are analysed among others. The abovementioned analysis enables us to address *de lege ferenda* in the later chapters, in particular while analysing the need and potential for the criminalisation of the offence of viewing child sexual abuse materials on the Internet as well as closing the gaps in legislation.

The problem of viewing child sexual abuse materials on the Internet, however, is of an interdisciplinary nature, thus interdisciplinary approach presets to be beneficial in answering research questions. Moreover, even when laws are in place, as it is, for example, in Sweden, the protection is not effective, thus there is a need to apply the socio-legal method alongside

¹⁰ Choice of these particular countries for the analysis is explained in the chapter 1.6 Delimitations.

with the dogmatic legal method. The use of socio-legal method provides a broader picture to the analysis of this thesis, thus makes it possible to give more clear answers for the research questions. Psychology and social studies are used as they can provide an understanding of triggers behind the obsession with child sexual abuse or exploitation materials, and might be also used in a treating of offenders.¹¹ Here, research and publications by Quayle and Taylor, Svedin and Back, Carr, and Gehl are used *inter alia*. As the issue of viewing child sexual abuse on the Internet is complicated by the wide use of technology, I use publications on the matter to clarify the terminology and present examples in order to provide the reader with the comprehensive view over the situation of viewing child sexual abuse materials on the Internet, and complications of the wide use by ICT. A study performed by Owen and Savage is being one of such examples as it not only demonstrates the statistics on viewing, but also illustrates the methods that can be used to perform investigations on hidden parts of the Internet.

The list of studies and publications mentioned in this subchapter is, of course, not a full one, and serves as an example to illustrate the types of materials I am working with in order to answer research questions of this thesis.

1.5.2 Theory

A wide use of technologies among the perpetrators creates a demand for an analysis from the perspective of relationship between law and technology¹², alongside with means and methods of ICT which can be used in the identification process which can be one of the main obstacles as it is noted by some researchers.¹³ The need for identification of subjects of a crime calls for rather broad surveillance mechanism, the mere idea of which comes hand in hand with the issue of interference with the private life of the individuals. This Foucauldian Panopticon, in which the crowd of anonymous on the Internet is replaced by a collection of separated

¹¹ It was noted that support from others provides a feeling of comfort and understanding, as well as a false justification of actions - see, for example, E. Quayle and M. Taylor in "Model of Problematic Internet Use in People with a Sexual Interest in Children", *Cyber Psychology and Behavior*, vol.6, N.1 (2003) cited in ECPAT Sverige "The Commercial Sexual Exploitation of Children" edited by H. Karlén (2011).

¹² The need for this, for example, had been pointed out by M. Hildebrandt "Law as Information in the Era of Data-Driven Agency" in "The Modern Law Review", vol. 79 (2016).

¹³ See, for example, M. Eneman "Internet Filtering – A legitimate control mechanism of criminal behaviour in the digital society?" (2016).

individuals,¹⁴ was, is and would be fiercely opposed by a principle of the protection of the fundamental rights such as privacy and fair trial, as it had recently happened in USA.¹⁵ Not only the notion of the private life is at stake in relation to the balance of rights, but also the freedom of expression, which had been widely used to justify the viewing and possessing child sexual abuse materials without engaging in distribution or production of thereof. Although, this had been challenged by case-law¹⁶, as well as by researches¹⁷, it still remains a lacuna that can be used by offenders in order to escape prosecution.

To oppose such views, the harm caused by viewing child sexual abuse materials to the victims is analysed during the scope of the thesis. Being one of the core elements in relation to criminalisation of a punishment-worthy conduct, harm also corresponds to the severity of the punishment in words of some researchers.¹⁸ Discussion on appropriate punishments for the crimes of viewing child sexual abuse materials on the Internet does not fall within the scope of this thesis. Still it appears important to address retributivism in relation to the effectiveness of protection offered by some national legislations. The inclusion of a *mens rea*, another important element in defining a criminal nature of the offence of viewing child sexual abuse materials helps to sort cases that span a wide range of human behavior and to provide some form of moral evaluation for different individuals and their actions.¹⁹

Moreover, the alleged harmlessness of the viewing of child sexual abuse materials affects the behavior of the perpetrators, who still are able to find a comfort in a peer support, and justify their actions as these are not real children, not even a person.²⁰ Such objectivization of a child

¹⁴ M. Foucault “Panopticism” Included in: “Discipline and Punish: The Birth of the Prison” (1991) [1979]

¹⁵ United States v. Michaud (2016); United States v. Walter E. Ackerman, appeal (2016).

¹⁶ See, for example, ECtHR case O’Carroll v. United Kingdom 41 EHRR SE1, ECtHR case of Karttunen v. Finland (2011), U.S. Supreme Court cases New York v. Ferber 458 US 747 (1982), Miller v. California 413 U.S. 15 (1973).

¹⁷ See, for example, Y. Akdeniz, N. Strossen “Sexually oriented expression” in Y. Akdeniz, C. Walker, D. Wall (eds) “The Internet, Law and Society”(2000), Harlow: Addison Wesley Longman , 207-31 cited by Y. Akdeniz in “Internet Child Pornography and the Law: National and International Responses” (2008), Ashgate Publishing Limited,, p. 4.

¹⁸ M. Matravers, “Is Twenty-First Century Punishment Post-Desert?,” in Tonry, Retributivism Has a Past: Has It a Future?, p30–45, cited by P. Tomlin “Retributivists! The Harm Principle Is Not for You!” (2014).

¹⁹ “Child Pornography, The Internet, and the Challenge of Updating Statutory Terms”, (2009), Harvard Law Review 2009/06/01, Vol: 122, p 2207.

²⁰ The argument, however, is used in relation to a materials of the sexual abuse of the real children as well, as one can see from the interviews with offenders taken during the course of COPINE project cited by E. Quayle, M. Taylor “Model of Problematic Internet Use in People with a Sexual Interest in Children” (2003): “. . . it wasn’t a person at all it was . . . it was just a flat image . . . it was a nothing”.

comes along with Kantian²¹ perspective, as children presented on materials are considered as mere objects, or means to fulfil the desire of a viewer to reach sexual climax. Such dehumanization of a real victim leads to prolonged suffering from the abuse itself as well as from its consequences. Moreover, objectivization further aggravates damage caused to child's integrity and dignity, that often leads to high levels of anxiety and negatively impacts child development. Therefore, as it was noted in R v. Sharpe cited by Akdeniz, criminalisation of child sexual abuse materials seek to prevent harm "*that flows from the very existence of images and words which degrade and dehumanize children*".²² Notably, it had been noticed by some, that raising awareness on the reality of the children that suffering from abuse in order to produce materials can contribute to crime prevention and decrease normalisation of consuming child sexual abuse materials.²³ Thus, to prevent further dehumanisation and objectivization of children.

The concept of moral, thus is also used during the course of the analysis and appears to be of importance for this thesis. One may claim that there is an agreement in international society that sexual abuse of children is immoral. Though not all the offences related to it are criminalised, and viewing of child sexual abuse or exploitation materials on the Internet being one of examples, it is still considered to be immoral to watch child pornography materials. Furthermore, the protection of morals is one of the grounds on which right to private life and freedom of expression can be limited. Therefore, the concept can be helpful in a discussion of balance between rights.

²¹ I. Kant "The metaphysical elements of ethics" (1780).

²² R v. Sharpe, 2001, SCC 2. File No 27376, 26 January 2001 cited by Y. Akdeniz in "Internet Child Pornography and the Law: National and International Responses" (2008)

²³ E. Quayle, M. Taylor "Child pornography and the Internet, perpetuating a cycle of abuse", Deviant Behavior, 23 (4) (2015).

1.6 Delimitations

This thesis seeks to explore the problem of viewing child sexual abuse materials on the Internet. Thus, it would be wise to start my delimitations with the notion of “materials”.

Materials vary in terms of video, photographs, pseudo photographs (a picture made of several other pictures), livestreams (videos which are not saving), and change with the rapid emergence of new technologies. However, since the nature of materials is not a focus of the thesis since it would not be wise to limit myself to the existing technologies, leaving children unprotected from the future developments. Yet it must be noted that modern computer tools allow to generate artificial images which are difficult to distinguish from the real photographs of real children. Such images are noted by some scholars to be covered by Budapest Convention, Lanzarote Convention, and even by OPSC under the notion of “whatever means”.²⁴ Therefore, to provide more broader protection of children rights, I would include the notion of computer-manipulated and computer-generated materials under the scope of child sexual abuse or exploitation materials. Same goes for art and animation of child sexual abuse as for the purposes of this thesis, the broader definition would be used to cover all types of the child sexual abuse materials.

It is wise to mention that materials can even be produced by children themselves (for example, during the process of “sexting” between two adolescents, or obtained by a paedophile tricking a child to take a photo or video of themselves), and quickly distributed on the Internet. Such materials are still largely considered to fall under the definition of child pornography. That, while being questioned by some scholars²⁵, would not be discussed during the course of this thesis.

It is important to keep in mind that regardless of the nature of creation of the materials, viewing and sharing these, as well as accessing them for the sexual purposes, traumatise the

²⁴ A. Gillespie, “Child Pornography: Law and Policy”, (2011), p. 104.

²⁵ For example, in UK, that, in turn, gives a rise to a legal collision when children commit criminal acts by taking pictures of themselves, as it is argued by Gillespie. See A. Gillespie, “Tinkering with Child Pornography” *Criminal Law Review* 3, (2003); A. Gillespie “Adolescents, Sexting and Human Rights” in *Human Rights Law Review*, 13 (4): 623-643 (2013); See also T. Buck “International Child Law” 2nd ed. (2011).

person that is depicted on the materials.²⁶ Moreover, as it was pointed out by Quayle, Taylor and Holland already in 2001, regardless of the content, each time that such materials are accessed for a sexual purpose, it victimises and dehumanises the individual concerned.²⁷

Regarding the issue of viewing, certain limitations must be set in relation to those who come across child pornography by chance. As it was noted by Gillespie, an element of *mens rea* would be required for criminalisation those who deliberately seek the materials.²⁸ Thus, by claiming that viewing of child sexual abuse materials should be criminalised, I mean only intentional viewing.

The problem is certainly much larger as viewing often is the first step in a process of starting a collection, participating in trade or exchange of images and committing an actual sexual abuse towards children. There are many situations when adults are actively participating in abuse using various technological tools, which make it significantly more difficult to identify offenders, the industry is growing rapidly, despite the attempts made by states to combat such crimes. Thus, I do not in any matter claim that these offences are less important or deserve less attention as most of them are criminalised in a large number of countries. It had been repeatedly said that, though the progress had been made, the problem remains, crimes are continuing to be committed and become more violent with the time. Consequently I argue that some ideas of this paper can be used in relation to most crimes of child sexual exploitation on the Internet. The paper, however, has its own limits, therefore the notion of viewing child sexual abuse materials on the Internet being a severe violation of human rights of children, is the main focus.

Factors which affect the consuming rate, sometimes even lead to the obsession, are also an important component of any analysis on the matter. Yet, as this thesis has a clear legal purpose, these factors are only mentioned briefly. Needless to say that social and behaviour studies present to be relevant for the purposes of the thesis, for example, to overcome some common arguments already in the first chapter. Same can be said on the psychological means and methods which can be used to work with the offenders and victims.

²⁶ See, for example, A. Gillespie “Adolescents, Sexting and Human Rights” in *Human Rights Law Review*, 13 (4): 623-643 (2013).

²⁷ E. Quayle, M. Taylor, G. Holland “Child Pornography, the Internet and Offending”, (2001).

²⁸ A. Gillespie “Child Pornography. Law and Policy” (2011), p. 39.

Interjurisdictional nature presents to be one of the most critical characteristics of the crime. The need for the combined action from the states had been pinpointed already during the introduction phase and are going to be addressed later on. The paper is set to explore the problem from different angles in relation to international, regional and national legal frameworks as it seems that actions taken on all levels will be the most effective in fighting such crimes. It would not be possible to analyse all existing legislation attempts in relation to child sexual abuse in this thesis, nor it seem necessary as it had already been performed several times by the International Centre for Missing & Exploited Children (ICMEC)²⁹. It seems only logical to partly base my research on this report as it not only analyses legislations, but also issued recommendations on changes which are necessary in combating crimes.

Thus, I use some national legislations as an examples to illustrate different aspects of the problem as well as different approaches taken by states in relation to child sexual abuse. For this research I've chosen Sweden, as there is a fairly recent statistics on downloading rates within the country alongside with the laws criminalising viewing child sexual abuse materials. At the same time, there is a statistics on prosecution rates clearly illustrating that existing legislation is not effective to protect children's rights. Simultaneously I examine the UK system as there is an effective tool for public to report child sexual abuse content of different kinds - Internet Watch Foundation³⁰. I address Russian legislation, as the country is a part of Council of Europe (CoE) and ratified major international and regional instruments on child sexual abuse. However, the notion of viewing the materials is not mentioned in national laws, which leads to horrifying statistics on the searches for child sexual abuse materials on Yandex - Russian-based search engine similar to Google.

Outside Europe, I examine practices of the US, as case-law there differs from those of the European Court of Human Rights (ECtHR) and Court of Justice of the European Union (CJEU). Moreover, the US remains not a party to the CRC, thus there is a need to address the status of some norms of CRC in relation states that are not party to it. I also use Canadian example of regulation the work of Internet service providers (ISPs) as a good practice in the

²⁹ "Child Pornography: Model Legislation & Global Review" International Centre for Missing & Exploited Children (2016).

³⁰ Internet Watch Foundation, available at: <https://www.iwf.org.uk/> (last visited 20 May 2017).

fourth chapter, as it is one of the rare working solutions in order to regulate ISPs activities and ensure protection of children's rights.

The reading and translation of materials on Russian and Swedish is done by me and based on my own understanding of these languages unless it is stated otherwise.

2. Chapter Two: Viewing Child Sexual Abuse Materials on the Internet as a Criminal Offence

2.1 Defining Child Sexual Abuse Materials

One of the main claims of this thesis is that viewing child sexual abuse or exploitation materials on the Internet is a crime. Thus, it would be wise to start with legal definitions of child pornography used in different instruments, and examine wide effects of viewing child sexual abuse materials on the Internet. Notably, as I mentioned earlier, the term “child pornography” is used more often to address such crimes, than those of “child sexual abuse” or “child sexual exploitation” which are recommended by ECPAT International³¹ as well as some scholars³².

Child pornography is defined in the Article 2 of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC). In accordance to the OPSC *“any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes”* constitute child pornography.

The definition is reflected also in regional instruments, such as for example, the EU Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography (Directive 2011/93): *“images of child sexual abuse, and other particularly serious forms of sexual abuse and sexual exploitation of children”*.³³ Another reflection can be found in The International Criminal Police Organization (INTERPOL) Specialists Group on Crimes against Children guidelines. Here sexual abuse materials are considered as *“the consequence of the*

³¹ ECPAT International in “Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse” (2016).

³² See, for example, A. Gillespie “The Sexual Offences Act 2003: Tinkering with “child pornography” (2004) quoted by M. Eneman in “Human Rights in the Digital Age”, edited by M. Klang and A. Murray (2005), p. 28, claiming that words “indecent” or “abusive” describe the material more clearly.

³³ Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011.

exploitation or sexual abuse perpetrated against a child. It can be defined as any means of depicting or promoting sexual abuse of a child, including print and/or audio, centred on sex acts or the genital organs of children".³⁴ Budapest Convention states that child pornography includes pornographic material that visually depicts "a minor engaged in sexually explicit conduct"³⁵, or "a person appearing to be a minor engaged in sexually explicit conduct, or realistic images representing a minor engaged in sexually explicit conduct"³⁶. Lanzarote Convention specifies that the term "child pornography" shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes³⁷. That includes, also, the notion of the sketches and drawings, as it is argued by Elena Martellozzo, thus allowing more broad protection against consumers of child sexual abuse materials.³⁸

Definitions mentioned above also refer to terms of child sexual abuse and exploitation. It is of importance, however, not to let the terminology disputes between scholars mislead us, when we are thinking about the content of a crime and its consequences. As it pointed out in EU Directive 2011/93 child pornography abuses constitute serious violations of fundamental rights, in particular of the rights of children to the protection and care necessary for their well-being, as provided for by the CRC and by the Charter of Fundamental Rights of the European Union. Thus the focus of this thesis remains on the phenomenon of viewing child sexual abuse materials on the Internet disregarding the terminology disputes.

³⁴ ECPAT International in "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse" adopted by the Interagency Working Group in Luxembourg, 28 January 2016.

³⁵ Budapest Convention Article 9 (2)(a).

³⁶ Budapest Convention Article 9 (2)(b).

³⁷ Lanzarote Convention Article 20(2).

³⁸ E. Martellozzo "Online Child Sexual Abuse. Grooming, Policing and Child Protection in a Multi-Media World" (2012).

2.2 Reflection of the Offences Related to Child Sexual Abuse Materials in International Legal Instruments

The issue of child sexual exploitation has been under the attention of the international community for some decades now, thus there is a number of NGOs working on the field, as well as international bodies. In his book “International Child Law” Trevor Buck takes a special notice in two bodies on the global level that featured the problems of child sexual abuse and exploitation on their respective agendas: the G8 and the UN,³⁹ CRC and the OPSC being the most prominent examples alongside with the establishment of the Special Rapporteur on the sale of children, child prostitution and child pornography. On the regional level Lanzarote Convention, Budapest Convention, African Charter on the Rights and Welfare of the Child can be named *inter alia*.⁴⁰ EU Directive on Combating the Sexual Abuse and sexual Exploitation of Children and Child Pornography, and EU Directive on Child Exploitation serve as another examples of the supra national instruments.

Criminalisation of the production, distribution, exportation, transmission, importation, intentional possession and advertising of child pornography was named as a tool in fighting child sexual abuse in the preamble to the OPSC, which refers to the International Conference on Combating Child Pornography on the Internet, held in Vienna in 1999. Previously cited EU Directive also addresses the need for the member states to criminalise at least the most serious forms of child sexual abuse, and protect victims.

That said, criminalisation of viewing child sexual exploitation materials is not mentioned explicitly in most instruments, its status remains unclear. Knowingly obtaining access, through information and communication technologies, to child pornography is only required to be considered as a criminal activity by state parties to the Lanzarote Convention. That is a step forward in order to close the gap in relation to viewing child sexual abuse materials, though the requirement to consider cannot be argued to be enough in order to secure children’s rights. Statistics illustrate the trend that lead to further dehumanisation of children

³⁹ T. Buck “International Child Law” 2nd ed. (2011), p. 265.

⁴⁰ Article 16 of the African Charter on the Rights and Welfare of the Child.

all over the world. As it can be seen from the ICMEC study, 50 of the examined countries still not criminalise both viewing and downloading child pornography.⁴¹ The number had grown by 9 countries since the first issue of the report.⁴²

The discussion on the issue is still ongoing, as it is still considered by some not to be a crime as there is no element of guilt and no harm coming from the process of watching. The arguments going as far as to suggest that watching child sexual abuse saves children from the real crimes, as paedophiles achieve their aims by simulation. Considering that this claim remains one of the strongest against criminalisation watching child sexual abuse materials, it requires more detailed analysis which is provided in next subchapters.

⁴¹ ICMEC “Child Pornography: Model Legislation & Global Review” (2016).

⁴² That, however, might be due to the growth of the number of countries examined and change of the methodology. As it is mentioned on the report, the 1st edition of this report looked at the legislation of the 184 INTERPOL member countries. Beginning from the 6th Edition, the report was expanded to look at the legislation of 196 countries. Regardless, the number still had grown from 7th to 8th (the last for now) edition.

2.3 Child Sexual Abuse materials on the Internet: Accessibility, Availability, Assortment

As it was previously pointed out, child pornography is not a new phenomenon, similarly to the child sexual abuse itself. Likewise it has long gone unnoticed by legislators and general public. Moreover, it took some time for the laws to be used in practice to investigate, prosecute and prevent crimes of child pornography. For example, in the United States, child sexual abuse first appeared in the federal Child Abuse Prevention and Treatment Act only in 1974.⁴³ At the same time during 1970s about 300,000-600,000 children under 16 years old had been involved in the production of pornographic material in the USA.⁴⁴ In Sweden, the law was amended to forbid the production and distribution of child pornography in 1980,⁴⁵ however, no materials had been confiscated up until a decade later, in the beginning of 1990's.⁴⁶ Still, materials had been largely produced, and Scandinavia remained one of the world leading regions on the market under 1980's,⁴⁷ photos and videos being sold and sent to the customers via mail. That way, however, became more and more risky with wider criminalisation of at least some aspects of child sexual exploitation, until the Internet came into the picture relatively at the same time the first paedophile mailing lists had been uncovered by police in different countries.

The beginning of massive use of the Internet largely affected the quality and quantity of the child sexual abuse materials. The spread of child sexual abuse materials has boosted significantly over the last decades, raising a worry among the legislators and civil society. It had been widely noted that distribution of the child sexual abuse materials became rather easy and incredibly profitable.⁴⁸ Thus, the EU Directive on Combating the Sexual Abuse and

⁴³ D.K. Weisberg, "The "Discovery" of Sexual Abuse: Experts' Role in Legal Policy Formation" Univ. of California Davis Law Review 18, 1-57 (1984) cited by M. Freeman in "The Moral Status of Children: Essays on the Rights of the Children" (1997) p. 257.

⁴⁴ C.G.Svedin, K. Back "Children who don't speak out. About children being used in child pornography", Rädna Barnen Sweden (1996), p. 11.

⁴⁵ *Ibid.*

⁴⁶ ECPAT Sverige and Jure Förlag AB, "The Commercial Sexual Exploitation of Children" edited by H. Karlen (2011) p. 44

⁴⁷ *Ibid.*

⁴⁸ See, for example, "14 months on: A combined report from the European Financial Coalition 2009-2010", available at <http://www.ceop.police.uk/efc/> cited at the ECPAT Sverige and Jure Förlag AB, "The Commercial Sexual Exploitation of Children" edited by H. Karlen (2011) p. 43.

sexual Exploitation of Children and Child Pornography reflects on the increasing rate of spread of child sexual abuse materials with the use of technologies, namely, the Internet.⁴⁹ Same goes for the OPSC, as already in the preamble, states parties have expressed their concern on the growing availability of child pornography on the Internet and other evolving technologies, and have been calling for action to eliminate all forms of child sexual exploitation and abuse.⁵⁰

Availability of the materials was named as one of the factors of emergence and growth of viewers and downloaders, who first act similar to voyeur.⁵¹ Since it is relatively easy to find child pornography on the Internet with a wide variety of images and videos available, there might be no need to save such a dangerous materials on one's computer, thus escaping prosecution in some countries. Yet their needs are increasing with time making them view or download more and more violent materials,⁵² raising a demand and a production of new material, that was pointed out by the UN Special Rapporteur on sale of children, child prostitution and child pornography.⁵³

Moreover, with the demand is increasing alongside with the amount of materials, violence of the abuses tends to raise.⁵⁴ As it was noted by Carl Göran Svedin and Kristina Back, "*there is a little similarity between the so-called "French postcards" and today's close-up pictures of advanced sexual acts*".⁵⁵ There is a growing tendency to violence among the "customers" who view the material to achieve an arousal and, eventually, to reach a climax. That encourage the "producers" to generate more and more graphic content. The words of Alex Wood, the police inspector that investigated the "Orchid Club" case in 1996 would be another example to this: "*the abuse I saw and heard was graphic, often photographed in stages, sometimes involving children as young as six months*".⁵⁶ Within more than twenty years

⁴⁹ Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011.

⁵⁰ Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography (2000).

⁵¹ Quayle, E. and Taylor, M. "Model of Problematic Internet Use in People with a Sexual Interest in Children" (2003).

⁵² *Ibid.*

⁵³ J.M. Petit "Rights of the Child: Report submitted by the UN Special Rapporteur on sale of children, child prostitution and child pornography" UN Economic and Social Council, 2004, E/CN.4/2005/78).

⁵⁴ See, for example, E. Quayle, M. Taylor, G. Holland "Child Pornography, the Internet and Offending", (2001). See also the trends in IWF Annual Report 2016, available at:

https://annualreport.iwf.org.uk/assets/pdf/iwf_report_2016.pdf (last visited 22 May 2017).

⁵⁵ C.G. Svedin and K. Back "Children who don't speak out. About children being used in child pornography." (1996) Rädna Barnen Sweden.

⁵⁶ ECPAT Sverige "The Commercial Sexual Exploitation of Children" edited by H. Karlen (2011).

passed since the Orchid Club had been uncovered, one can only imagine how far the fantasies can reach nowadays.⁵⁷

⁵⁷ To provide an example, one can refer to one of the offenders, convicted of downloading child sexual abuse materials, interviews during the COPINE project and cited by E. Quayle, M. Taylor and cited in “Model of Problematic Internet Use in People with a Sexual Interest in Children” (2003), “*I was actually getting quite bored as it were . . . erm . . . with the sort of child pornography . . . I was becoming sort of much more obsessed with bondage ... and sort of torture . . . imagery. So . . . I'd kind of exhausted . . . the potential that it had for sexual arousal*”.

2.4 Imitation, Stimulation or Inspiration: Relations Between Child Pornography and Child Sexual Abuse

2.4.1 Models on Relationship Between Pornography and Sexual Crimes

It would be wise to mention that the question on the connection between watching pornography and committing sexual abuse is again not a new one, and had been discussed over a few decades now. The research on the issue had been performed as early as during the late 1970's in the USA and resulted in the adoption of a so-called "catharsis model", as it is mentioned by Svedin and Back.⁵⁸ The studies at the time considered that there is an inverse relationship between sexual crime and availability of pornography. The model, however, was replaced by an "imitation model" during the later years, as the connection between pornography, sexual violence and sexual abuse had been established at the late 1980's.⁵⁹ Since then there had been numerous reports showing that pornography had indeed influenced the perpetrators of sexual crimes,⁶⁰ and had also been used to coerce children into submission or justify the acts so the children see it as acceptable behavior.⁶¹ Statistics are also contributing to the "imitation model" argument. Thus, already in 2003, the study showed that two-thirds of the people arrested for child sexual abuses, possessed a significant collections of child pornography materials.⁶² Other studies show that only in Sweden 48% of those charged

⁵⁸ C.G. Svedin and K. Back "Children who don't speak out. About children being used in child pornography" (1996), p. 17.

⁵⁹ M.H. Silbert, A.M. Pines "Pornography and Sexual Abuse of Women" (1984) cited by C.G.Svedin, K. Back "Children who don't speak out. About children being used in child pornography", Rädta Barnen Sweden (1996), p. 18.

⁶⁰ See, for example, G.G. Abel "Use of pornography and erotica by sex offenders. Paper presented to the United States Attorney General's Commission on Pornography" (1985) cited by C.G.Svedin, K. Back "Children who don't speak out. About children being used in child pornography", Rädta Barnen Sweden (1996), p. 18.

⁶¹ These are also the means using by paedophiles for "grooming" of children on the Internet so that they will engage in a sexual relationship with the perpetrator.

⁶² J. Wolak, K. Mitchell, D. Finkelhor "Internet Sex Crimes Against Minors: The Response of Law Enforcement", Crimes Against Children Research Center (2003) cited by M. Eneman in "Human Rights in the Digital Age", edited by M. Klang and A. Murray (2005), p. 36.

with possession of child pornography are also charged with other sexual crimes against children⁶³, in the USA in 2011 the number was 41%.⁶⁴

2.4.2 From Viewing to Abusing

There are a few factors contributing to the risk of going all the way from viewing child sexual abuse materials to committing a sexual abuse of a child, however, it is not a purpose of this thesis to analyse them all in detail. Nevertheless it seems logical to mention at least some of them before proceeding to the next part, as it is also an important piece of the argument for criminalising watching child sexual abuse and taking an immediate action to protect the rights of the children.

The materials are often distributed in paedophile networks, mostly located on the dark web. While there is a large amount of materials available, networks provide with more opportunities such as, for example, to exchange the experiences or actively participate in abuse using technological tools. To enter a paedophile ring, one is often required to provide some new materials, the number of which can be astonishing⁶⁵. It seems only logical to claim that such requirements indeed increase the risk of committing a child sexual abuse. Moreover, the Internet provides unprecedented opportunities for paedophiles to connect with children, which, as it was pointed out by Swedish scholar Marie Eneman, in turn increase the number of children available compared to the real life as there are no geographical limitations and less social exposure.⁶⁶ Thus, the requirements for the new material can now be larger than it had been two decades ago in the Wonderland Club.⁶⁷

⁶³ “Barnpornografibrottet. Det straffrättsliga skyddet mot dokumenterade sexuella övergrepp mot barn”, ECPAT Sverige (2017), available (in Swedish) at: http://www.ecpat.se/uploads/ECPAT_Barnpornografibrottet_2017.pdf

⁶⁴ “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (2016).

⁶⁵ For example, to obtain membership in the Wonderland Club - a paedophile ring which had been uncovered in 1998, one should have contributed with 10 000 unique child pornographic pictures, as it is mentioned in ECPAT Sverige and Jure Förlag AB, “The Commercial Sexual Exploitation of Children” edited by H. Karlen (2011) p. 53.

⁶⁶ M. Eneman in “Human Rights in the Digital Age”, edited by M. Klang and A. Murray (2005), p. 31.

⁶⁷ As an example one can refer to numbers from Swedish Police provided at ECPAT Sverige and Jure Förlag AB, “The Commercial Sexual Exploitation of Children” edited by H. Karlen (2011) p. 47, namely, that in 2002 a large criminal case on child sexual abuse could consist of approximately 20,000-25,000 pictures. In 2011 there had been several cases of more than one million pictures.

2.4.3 Psychological factors linking offences of child sexual abuse

However, it is not only such requirements which lead to increasing rate of child sexual abuses. Sometimes, there is no need to exchange pictures or videos as paedophiles are finding a comfort and safety in connecting to each other. With the issue of child sexual abuse being brought to the public attention by the media for several decades, paedophiles often feel isolated or afraid to reveal the nature of their desires during their everyday life. The feeling of anonymity on the Internet only contribute to the willingness for paedophiles to engage in conversation with the people with the same interests. In such groups one can find support and understanding from the peers. That claim had been confirmed by the offenders themselves during the interviews referred by Quayle and Taylor: *“Ah . . . that felt good . . . to be me . . . with amongst what I then would consider to be the only people that would really understand me. The only people I can be me with . . . they won’t judge me. They feel the same way. We’ve got so much in common. I can feel . . . I fit in here”*.⁶⁸

Being part of a group presents to be rather important issue in normalisation of the sexual desire towards minors and obtaining a false justification of the actions of all types from watching, sharing, exchanging or downloading (“we are not harming real children”) to committing an actual sexual abuse towards a child (“if they are doing it on the videos, then it might be okay to do the same”). As it is mentioned in the Explanatory Report to the Convention on Cybercrime (2001), it is widely believed that the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children.⁶⁹

Curiosity is often used by the perpetrators as an excuse justifying the first experience with child sexual abuse materials. However, what often starts with curiosity, can lead to the addiction once a person realises how easy it is to find child sexual abuse materials, and how

⁶⁸ E. Quayle, M. Taylor “Model of Problematic Internet Use in People with a Sexual Interest in Children” (2003).

⁶⁹ Explanatory Report, Budapest Convention on Cybercrime, 2001 ETS No 185.

safe it might feel due to the nature of the Internet. As with other obsessions, a person fixates on the issue, keeps looking for the new materials when online and when it's possible, thinks about it during the time spent offline. Again, here the evidences from the interviews with the offenders can be used as an example: *“Every opportunity that I had to get online when my wife wasn't in I would do it”*.⁷⁰

A desire to test boundaries is another factor leading to exploration of child sexual abuse materials. The feeling of anonymity largely affects Internet users as it creates a possibility to hide one's true identity (at least in the eyes of the offender), thus to avoid personal responsibility⁷¹ for the actions known to be illegal. As it was noticed by Taylor, Quayle and Holland, knowledge of the risks being taken can also serve to heighten arousal.⁷² The feeling of control of the situation and empowerment add to the desire to get more and more material, to engage in community, and eventually start collecting and exchanging materials.

Nevertheless, despite the different reasons people can come to viewing child sexual exploitation materials on the Internet, it should be kept in mind, that for many paedophiles the consumption of child pornography is indeed just a primary stage before committing a “real-life” child abuse.⁷³ It is not the purpose of this thesis to analyse the process from viewing to abusing, as it was done before. The main focus still remains on the viewing child sexual abuse materials being an offence on its own, that violates human rights and damages children. The next logical question, however, is how harmful the consumption of child sexual abuse materials whether with or without storing them on one's computer can be for the children themselves. To understand the matter one should analyse if there is any victim to crimes of that type, and if yes, what are the effects of reappearing materials on the Internet for these victims. This issue is examined in the coming subchapter.

⁷⁰ E. Quayle and M. Taylor “Model of Problematic Internet Use in People with a Sexual Interest in Children” (2003).

⁷¹ S. Turkle, *Life on the screen: identity in the age of the Internet* (New York: Simon and Schuster, 1995), cited by E. Quayle, M. Taylor, G. Holland in “Child Pornography, the Internet and Offending” (2001).

⁷² E. Quayle, M. Taylor, G. Holland in “Child Pornography, the Internet and Offending” (2001).

⁷³ K. Lanning, Presentation at the Fifth COPINE Conference, Cork, Ireland (2004), cited by M. Eneman in “Human Rights in the Digital Age”, edited by M. Klang and A. Murray (2005), p. 37.

2.5 No Victim, No Harm, No Guilt

The crime of viewing child sexual abuse materials was for a long time considered to be harmless and victimless. The notion is still present, not only among offenders⁷⁴, but in general public and judicial entities.⁷⁵ That, in turn, gives a rise for a significant concern as such views dehumanise a victim, which is often a real child suffering from the consequences of the offence. Thus, it seems important to examine the issue of the existence of a victim in this type of crimes alongside with the notion of harm caused by such conduct.

It is not necessary that users who view the materials of child sexual abuse come in any contact with real children, at least on the first stages of the obsession. Nor is it necessary that viewers are participating in the distribution of materials or even storing them. However, does it mean that there is no victim if there is no contact between an offender and a child? The answer, though, largely oversimplified, would be “no”. The child that is being sexually exploited in sake of a sexual pleasure of an adult, still remains a victim, even though in this case, adult is merely viewing the materials. As it was noticed by Gillespie, any materials on which one is presented on an intimate way are private by very nature, and even consented individual may be embarrassed if these are seen and distributed more widely than initially intended.⁷⁶ It is only logical to conclude that for a person which had been sexually abused as a child, the consequences would be much broader. First comes physical abuse, then psychological, which is repeated numerous times as long as materials are circulating on the Internet. This, as some suggested, can lead to secondary victimisation as a child has to come to terms with the fact that these images are perpetually circulating and that some will use these images for the purposes of sexual gratification.⁷⁷ It had been pointed out by Taylor and

⁷⁴ Citing interviews from the COPINE project by E. Quayle, M. Taylor in “Model of Problematic Internet Use in People with a Sexual Interest in Children” (2003), “. . . it wasn't a person at all it was . . . it was just a flat image . . . it was a nothing”; “But the big thing I kept saying and I believed it . . . with every inch of my body . . . was that this was OK because I'm not touching . . . I'm not touching anybody . . . it's better for me to sit here fantasizing and looking at pictures . . . and I'm not I'm not doing anything else”.

⁷⁵ Thus, the study conducted by Edwards in UK in 2001 showed that judges failed to recognise the danger of child pornography offences which resulted in the very short sentences, as it is mentioned by E. Martellozzo in “Online Child Sexual Abuse. Grooming, Policing and Child Protection in a Multi-Media World” (2012).

⁷⁶ A. Gillespie “Adolescents, Sexting and Human Rights” (2013).

⁷⁷ T. Palmer, Just One Click: Sexual Abuse of Children and Young People Through the Internet and Mobile Telephone Technology (London: Barnado's, 2004) cited by A. Gillespie “Adolescents, Sexting and Human Rights” (2013)

Quayle, there is a large chance that such materials would be in permanent circulation for a long time (one can even speak in terms of as long as the Internet, as we know it, exists, or perhaps, even longer) as once they are placed on the Internet they are quickly downloaded, mirrored and distributed.⁷⁸

In relation to effect on the victims, there is a strong need to point out, that multiple studies on the subject had been conducted over past few decades. These studies demonstrated *inter alia* that children exploited in child pornography showed feelings of isolation, anxiety and fear, had little trust in adults, negative self-esteem. Years later after the abuse, their feelings had been further traumatised by desperation, hopelessness and psychological paralysis.⁷⁹ They are still afraid that someone would find out or recognise them on the materials, and will make a judgement on them, feeling that they were willingly involved in the activities.⁸⁰ Notably, in 1980's it was much easier to eradicate the copies of materials, than it became during the Internet era. Modern research suggest that findings of such materials can lead to bullying and harassment among adolescents.⁸¹ In some extreme cases that had even led to suicide.⁸² The feelings of shame and guilt these children felt, the denial and a fear of someone they know seeing these materials show the effect of trauma being re-enforced every time the materials are being viewed. The consequences, which can be rather serious, even permanent, clearly demonstrate the graveness of the problem. Thus, there is a need to establish a theoretical basis for criminalising the offences of viewing child sexual abuse or exploitation material on the Internet, which are addressed in the following subchapter.

⁷⁸ See Taylor and Quayle, "Child Pornography: An Internet Crime" (2003) cited by A. Gillespie "Adolescents, Sexting and Human Rights" (2013).

⁷⁹ M.H. Silbert, "The Effects on Juveniles of Being Used for Pornography and Prostitution. Child Pornography and Sex Rights". In D. Zillmann and J. Bryant (eds), "Pornography: Research Advances and Policy Considerations". Hillside, NJ: Lawrence Erlbaum Press (1989) cited by C.G.Svedin, K. Back "Children who don't speak out. About children being used in child pornogprahy", Rädga Barnen Sweden (1996).

⁸⁰ T. Palmer "Behind the Screen: Children who are the Subjects of Abusive Images" in E. Quayle, M. Taylor "Viewing Child Pornography on the Internet" cited by T. Buck "International Child Law" 2nd ed. (2011), p. 264.

⁸¹ See Calvert, "Sex, Cell Phones, Privacy and the First Amendment: When Children become Child Pornographers and the Lolita Effect Undermines the Law" (2009) *CommLaw Conspectus* 1 at 13 cited by A. Gillespie in "Adolescents, Sexting and Human Rights" (2013).

⁸² See Albury and Crawford "Sexting, Consent and Young People's Ethics: Beyond Megan's Story" (2012) *Continuum: Journal of Media and Cultural Studies* 463 at 463 cited by A. Gillespie in "Adolescents, Sexting and Human Rights" (2013).

2.6 Criminalisation of Viewing: Harm Principle and *Mens Rea*

2.6.1 Consequences of viewing child sexual abuse materials for children

It seems relevant to finish that chapter with justification of the claim that the activity of viewing should be criminalised. To set a limit, only those who deliberately search and view child sexual abuse materials on the Internet, sometimes with the use of special technological tools that make it more difficult for law enforcement agencies to disclose the location of the user, should be prosecuted.

Viewing child sexual abuse and exploitation materials, as I argued during the course of this thesis, is not only an immoral activity. Child sexual abuse materials are documentation of the crimes against children, violations of their rights to dignity, wellbeing and health. Here, it would be wise to reflect the words of Quayle and Taylor, claiming that unlike the adult pornography which might involve consent of grown up individuals, child pornography is based upon the degradation, assault and sexual violation of children by adults - there can be no question of voluntary participation.⁸³ Indeed on such materials, whether it is a still (photo images, pseudo photographs made of parts of several other pictures) or moving (films, real time videos) the real children are still abused, sometimes to the point of torture, their rights being gravely violated for the sexual pleasure of random adults. Coming back to the example, I used as an epigraph to this chapter, child's tears and pain are among the aims of the whole process for paedophiles, as well as humiliation which doesn't stop with the end of the video or click of the camera. Every time the materials are displayed, the trauma of child sexual abuse is reinforced.⁸⁴ The more times materials are viewed, the larger is the scope of

⁸³ E. Quayle, M. Taylor "Child Pornography: An Internet Crime" (2003) cited by M. Eneman in "Human Rights in the Digital Age", edited by M. Klang and A. Murray (2005).

⁸⁴ A. Gillespie, "Adolescents, sexting and human rights" in Human Rights Law Review, 13 (4): 623-643 (2013); M. Eneman in "Human Rights in the Digital Age", edited by M. Klang and A. Murray (2005); Palmer, "Just One Click: Sexual Abuse of Children and Young People Through the Internet and Mobile Telephone Technology", London: Barnado's, (2004).

dehumanization of a real child. As it was mentioned before, studies showed that circulation of child sexual abuse materials on the Internet can also lead to anxiety, fear of humiliation (and a real humiliation) and other severe consequences for the victim, thus there is a real harm being caused. The question, however, would this harm be enough to justify the criminalisation and punishment of the viewer? To analyse this, one should take a close look at the notion of the harm principle.

2.6.2 Harm Principle

There are two basic retributive principles, as it was pointed out by Hugo Bedau in 1984.⁸⁵ First is that the severity of the punishment must be proportional to the gravity of the offence. That is not a relevant for this thesis, as it is not among aims of the paper to define the severity of the punishment for viewing child sexual abuse or exploitation materials on the Internet, though one can point out some questionable placements of child sexual abuse offences in some legislations. Instead, the focus of this subchapter would be on the second one which claims that only harmful actions should be punished.

Harm principle derives from the idea that, because punishment harms the offender, it can only be justified if it prevents greater harms.⁸⁶ The concept is incorporated into the ideas of legitimising State's interference with the rights of its nationals in order to protect the rights of others and prevent future human rights violations. For example, the right to private life and freedom of expression/speech that are actively being used as counterarguments in relation to criminalisation of viewing child sexual abuse materials, can be limited under the legitimate aims such as the need to protect rights of others. As it was previously noted, child sexual abuse is largely considered to be an act that severely violates human dignity and integrity of a victim among other rights of a child being subjected to crime. Another reasoning to limit these rights would be in order to protect morals. Violations do not end with the actual abuse, dehumanization continues as long as materials are being watched by others, and might have a wide effect on public morals. Normalisation of viewing child sexual abuse can lead to

⁸⁵ H. A. Bedau, "Classification-Based Sentencing: Some Conceptual and Ethical Problems," *New England Journal of Criminal and Civil Confinement* 10 (1984): 1–26, 13.

⁸⁶ A. Ripstein, "Beyond the Harm Principle" (2006), In: *Philosophy & Public Affairs*, 7/1/2006, Vol. 34, Issue 3, p. 215-245.

normalisation of child sexual abuse as it was illustrated by studies and interviews with the offenders.⁸⁷

Thus, referring to the discussion on the balance of rights, it can be justified to criminalise child pornography offences to the extent of deliberate viewing the materials, as such activities violate rights of the child, protection of which is secured under the international and national legal regimes. Some of the actions in child sexual abuse and exploitation amount to torture, prohibition of which has the status of *jus cogens* norm in international law.

The notion of the relations between the harm principle and retributivism had been on the philosophical debate for a long time. Kant, as it was pointed out by Hampton, suggested that these are consistent and mutually supportive as retributivism responds for the same violations of those individual rights that are also part of the moral foundation for the harm principle.⁸⁸ The practical expression of this can be found in many national legislations, including Swedish and Finnish, in which harm is a necessary element of a punishment-worthy conduct, accordingly criminal punishments should be proportionate to the harmfulness of actions.⁸⁹ Notably, in Sweden, crimes of child pornography, are considered to be crimes against a state order, not sex crimes, with the highest punishment normally being up to two years in prison or a fine.⁹⁰ That, as argued by Patrick Tomlin, goes along⁹¹ with the famous “Nozick formula” in which a deserved punishment is a function of harm and the responsibility of the offender.⁹² Tomlin, however, argues that these two concepts have nothing in common, and such an idea can lead to some dangerous consequences. Such as, for example, the situation with viewers of child sexual abuse, that largely escape punishment, or come to the knowledge of relatively cheap price of crime - the fine they simply need to pay off in case of being caught and prosecuted. That, as I claim during the course of this thesis, cannot be considered as an

⁸⁷ See, for example, E. Quayle and M. Taylor “Child pornography and the Internet, perpetuating a cycle of abuse” (2015).

⁸⁸ J. Hampton, “How You Can Be Both a Liberal and a Retributivist,” *Arizona Law Review* 37 (1995): 105–16, 106 cited by P. Tomlin in “Retributivists! The Harm Principle Is Not for You!” *Ethics* 124 (2014): 272–298.

⁸⁹ P. Tomlin in “Retributivists! The Harm Principle Is Not for You!”.

⁹⁰ It can, though, go up to the six years imprisonment in some aggravated circumstances or six months in some other cases. See, *Brottsbalk*, Chapter 16 para 10a, SFS nr: 1962:700.

⁹¹ P. Tomlin in “Retributivists! The Harm Principle Is Not for You!” citing also Andrew von Hirsch, “Censure and Sanctions” Oxford: Clarendon, (1993), 90–91.

⁹² Robert Nozick, “Anarchy, State and Utopia”, New York: Basic Books, (1974), 60–62.

effective protection of children's rights, as the prolonged harm caused for children remains unaddressed, and the vast majority of the offenders escape prosecution.⁹³

2.6.3 Mens rea: Deliberate Search For Child Sexual Abuse Materials and the Element of Knowing

It is becoming harder to deny that the harm caused by viewing child sexual abuse material on the Internet is substantial and severe for the victims of documented child sexual abuse, which is what these materials actually are. Still, the new question arises in relation to criminalisation of viewers of child sexual abuse materials on the Internet, namely the notion of *mens rea* which is incorporated in many national legislations in order to identify those who deliberately search for child sexual abuse materials. It is not enough for the person to see the materials, thus - for the offence to exist - to claim that someone had deliberately committed a crime of viewing child sexual abuse materials. There is a necessary element of will to search, find or receive and view such materials. Thus, in some national legislations not only an intent to view child sexual abuse materials is required, but also a knowledge that the email attachment or the website is or is likely to contain such materials.⁹⁴ It was even claimed that in the US the element of knowledge is an essential to protect those who received child pornography by mistake.⁹⁵

In the UK making an indecent image is a punishable offence in accordance to the provisions of the Protection of Children Act. The case-law equates downloading of child sexual abuse materials to an act of making an indecent image.⁹⁶ Moreover, the person may be found guilty of an offence of making an indecent image when opening attachment which is likely to contain an indecent image.⁹⁷ That, however, would only be true, if the person should have known that the attachment is likely to contain an indecent image. Hence, there is an element of knowledge needed to find a person guilty. An accidental viewing of child sexual abuse materials such as, for example, pop-ups or other form of advertisement, should not be

⁹³ As one can see from the statistics of Aftonbladet and Svenska Dagbladet study.

⁹⁴ R. v. Smith; R v. Jayson (2003);

⁹⁵ See, United States v. Osborne, 935 F.2d 32, 34 n.2 (4th Cir. 1991) cited in "Child Pornography, The Internet, and the Challenge of Updating Statutory Terms", (2009), Harvard Law Review 2009/06/01, Vol: 122, p 2209

⁹⁶ See R. v. Smith; R v. Jayson (2003).

⁹⁷ R. v. Smith; R v. Jayson (2003) cited by A. Gillespie in "Child Pornography: Law and Policy" (2011).

punishable, whereas “clicking” on the advertisement to see the materials would be considered as a deliberate act. Technology, however, complicates this formula as it is known for images to be stored in the cache without any intent from the user. Thus, an image from the pop-up advertisement may be stored in the cache, and discovered much later as it happened in *R v. Harrison* (2008) where the Court, in words of Gillespie, focused on the photographs rather than on the actions of a person.⁹⁸ Nevertheless, it would be of importance to point out that images from cache are still accessible for the user, thus capable of being in possession, as it was noted in yet another case.⁹⁹

There are, however, means and methods that allow to distinguish between intentional searching or opening the materials, and accidental viewing an advertisement, such as the data from service providers. It is possible and, in fact, recommended¹⁰⁰ to use special software to clean the cache in case of accidental viewing of child sexual abuse or exploitation materials, as well as report it in accordance with the instructions, provided by law enforcement agencies and NGOs.¹⁰¹ Still, even if one cleans the cache or uses “incognito” mode offered by some browsers such as, for example, Google Chrome, the input information can be available by ISPs. Thus it is possible to discover a trend in user’s online behaviour and distinguish those who deliberately search for child sexual abuse or exploitation materials.

Yet, it might be of interest to note here, that during my research on the problem that had been performed for more than seven months at the moment of submitting the thesis, I have not come across to links for child pornography resources, advertisements or pop-ups, not to mention the real materials. It is, of course, not enough to claim that such event is not possible, however, it can be used as an addition to the argument that there is a need to perform a certain actions to find child sexual abuse materials on the Internet. Still, the problem remains, as it these actions are relatively easy, and instructions are widely available (and these I had seen during the course of the research). Thus, it is not sufficient to barely claim that viewing child sexual abuse materials is a criminal offence. There is a need for a strong protection which

⁹⁸ A. Gillespie, “Child Pornography: Law and Policy” (2011), p. 125-126.

⁹⁹ *R v. Porter* (2006) discussed by A. Gillespie in “Child Pornography: Law and Policy” (2011).

¹⁰⁰ See, for example, A. Gillespie in “Child Pornography: Law and Policy” (2011).

¹⁰¹ For example, CEOP in the UK, available at: <https://www.ceop.police.uk/safety-centre/> (last visited 17 May 2017).

Or Virtual Global Task Force, available at: <http://virtualglobaltaskforce.com/> (last visited 17 May 2017).

would not be possible without analysing complications coming up from the global nature of the problem, that is examined in the next chapter.

3 Chapter Three: Viewing Child Sexual Abuse Materials on the Internet as a Global Problem

3.1 Child Sexual Abuse Materials on the Internet: Globalisation and Collective Efforts

A child from Switzerland is abducted and brought to Angola where she is filmed in a sexually explicit manner. The person filming these acts is a Barbados national. His accomplice, an Australian national, then takes the film and travels to Namibia where he uploads it to the Dark Web. From this point, paedophiles from St. Lucia, Italy, the United States, and countless other countries worldwide have access to this film through the Dark Web.

Which country is responsible for prosecuting this crime?¹⁰²

This example, used by Amanda Haasz, illustrates the wide, multinational nature of a crime of viewing child sexual abuse. Here, it is even aggravated by the issue of child trafficking. It might, however, be simpler, as the materials are produced at home by one or both of the child parents, who share the materials with some paedophile located in a different country, who then uploads it to the so-called dark web where the materials would be available for thousands of paedophiles from all over the world. With the rapid growth of the number of material and technologies protecting anonymity on the Internet, problem had been labelled by

¹⁰² A. Haasz, “Underneath It All: Policing International Child Pornography on the Dark Web” (2016), In Syracuse Journal of International Law & Commerce. Spring 2016, Vol. 43 Issue 2, p. 353-380.

many agencies as of international proportions.¹⁰³ There had been reported a significant increase in paedophiles viewing materials located in another country.¹⁰⁴

To set another example, even the possession of child pornography is not clearly prohibited by the CRC. Thus, Buck expresses his doubts in wording of the Article 3(1) of OPSC in regard to the criminalisation of the possession,¹⁰⁵ and points out that similar worries had been expressed by the Committee on the Rights of the Child (CtRC) and the Special Rapporteur, that called also for criminalisation of those who knowingly access or watch material online.¹⁰⁶ In absence of consistent legislation among the states, however, the problem of dual criminality arises, since, as it was pointed by Buck, the crime must be illegal in both the country that is to try the offence, and the country where the act took place.¹⁰⁷ The more states are included in this equation, the larger is the chance that there would be differences in legislation.

Notably, the legitimacy of the content is also considered to be the matter of jurisdiction. As an example used by Owen and Savage, whistleblowers sites are often considered legal, but may not be if used to disclose classified documents or by persons in repressive regimes.¹⁰⁸ The problem one should keep in mind, that child sexual abuse and child pornography are not considered to be a crime in relatively many states, though they may be considered to be at least immoral. Thus, there is a collision between national legislation which calls for more active measures taken by the states. It had been even said that the legislations differ so much that it is not possible for law enforcement agencies to act across borders,¹⁰⁹ and there is a need for broader international cooperation.

This chapter is aimed to emphasise that the problem is a global one, thus there is a need for collective efforts. Multinational nature makes it difficult to investigate and even harder to

¹⁰³ See, for example, INTERPOL on Crimes against children, available at: <https://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children> (last visited 20 May 2017).

¹⁰⁴ Global Alliance Against Child Sexual Abuse Online “2015 Threat Assessment Report” (2015).

¹⁰⁵ T. Buck “International Child Law” 2nd ed. (2011), p. 276.

¹⁰⁶ N.M. Maala, Report submitted by the Special Rapporteur on the sale of children, child prostitution and child pornography (2009) A/HRC/12/23.

¹⁰⁷ T. Buck “International Child Law” 2nd ed. (2011), p. 279.

¹⁰⁸ G. Owen, N. Savage “The Tor Dark Net” (2015), Centre for International Governance Innovation and the Royal Institute of International Affairs, available at: https://www.ourinternet.org/sites/default/files/publications/no20_0.pdf (last visited 05 May 2017).

¹⁰⁹ E. Martellozzo “Online Child Sexual Abuse. Grooming, Policing and Child Protection in a Multi-Media World” (2012).

prosecute such cases. The issue in question has been addressed by scholars,¹¹⁰ states, NGOs and international crime prevention agencies such as International Criminal Police Organisation (INTERPOL), and some steps had been done to protect rights of children. Thus, I would analyse the existing international, regional and some national legislation and practices to show how the work with this types of crimes is performed as well as what are the legal grounds for the actions. Still, I would argue from the perspective of child rights that what is done is not enough, since the issue of viewing without downloading the materials is often left behind, creating a possibility for paedophiles to consume large amounts of child pornography.

It is also important to notice the special nature of investigations on the Internet that comes with a particular amount of concerns such as potential violations of the right to private life and freedom of expression alongside with abuse of power by some states. Such fears certainly have a reason as there had been signs that states indeed can perform mass surveillance on entire population. One cannot, however, completely disregard the means and methods used to detect the offenders on the Internet as it will leave children without any real protection. There is a need to mention a problem of balancing the rights. Thus, to fully understand the issues in stake one should start with the concept of the dark web, tools to access it, and complications arising during the process of investigating offences committed by anonymous.

¹¹⁰ See, for example, A. Gillan "Race to Save New Victims of Child Pornography" (2003) cited by E. Martellozzo "Online Child Sexual Abuse. Grooming, Policing and Child Protection in a Multi-Media World" (2012).

3.2 The Complexity and Complications of the Dark Web

3.2.1 What is the Dark Web

To understand all the implications of the dark web for the problem of viewing child sexual abuse materials on the Internet, one should perhaps start with terminology. Thus, there are three parts of the Internet.¹¹¹ The first one is called “*the surface web*” that includes everything that can be found using search engines like Google or Yahoo. Next comes “*the deep web*” - the materials that cannot be found by search engines. It is important to keep in mind here, that deep web resources are not necessarily illicit, in fact most of the content is fairly legal. It includes also links and information that can only be reached through the search on the website (for example, the court case databases or someone’s bank account webpage). “*The dark web*” or “*darknet*” is a specific section of the Internet which is intentionally hidden and can only be accessed through the special software. While being hidden, the dark web is relatively easy to find. It can be accessible from every corner of the world as long as the person has the software (which can be easily downloaded) and knows how to navigate the darknet (for that there are many instructions on the surface web)¹¹².

The most prominent example of software used to access the darknet is The Onion Router (Tor) browser, which is officially aimed to improve people’s privacy and security on the Internet.¹¹³ In itself, what Tor is doing is not illegal, moreover it can be used for the protection of human rights all over the world. With the use of special tools, called “the onion technology”, Tor hides the location of the user, allowing to overcome a censorship¹¹⁴ or prevent websites from tracking the person or their family members, thus saving lives of

¹¹¹ Clearing Up Confusion - Deep Web Vs. Dark Web, BrightPlanet (2014), available at: <http://www.brightplanet.com/2014/03/clearing-confusion-deep-web-vs-darkweb/> (last visited 26 April 2017).

¹¹² The search on Google “how to access the darknet” comes up with 2 820 000 results (last checked 26 April 2017).

¹¹³ According to the information from the official website of the TOR project, available at: <https://www.torproject.org/about/overview> (last visited 26 April 2017).

¹¹⁴ This, for example, is used by Chinese Internet users to overcome “The Great Firewall” - the state censorship system which is blocking access to western websites from China. See, for example, Human Rights Watch report “Race to the Bottom”. Corporate Complicity in Chinese Internet Censorship” (2006) Volume 18, No. 8(C), available at: https://www.hrw.org/reports/2006/china0806/3.htm#_Toc142395820 (last visited 26 April 2017).

domestic violence victims¹¹⁵ and protecting whistleblowers¹¹⁶. It is said that Tor can even be a helpful tool to law enforcement agents in operations to uncover illicit activities on the darknet, including paedophile rings.¹¹⁷

3.2.2 Possibilities and Potentials to Control the Dark Web

Technology protecting both hosts and visitors of the websites¹¹⁸ poses significant difficulties for the law enforcement to investigate offences and prosecute those using the dark web for illegal purposes. Despite all the good intentions, Tor is being actively used to protect anonymity of those who operate the Internet black market¹¹⁹, where one can easily find illicit content including child sexual abuse materials.¹²⁰ Remarkably, a study committed by Gareth Owen and Nick Savage found that sites hosting child abuse imagery were the most frequently requested.¹²¹ In twelve days observed, there had been more than 168,000 requests per day on child sexual abuse websites.¹²² In contrast, Silk Road, the most famous black market website, which got a lot of public attention for the last few years, had less than 10,000 requests. While there are several possibilities of misleading in these figures, recognised by authors, the

¹¹⁵ R. W. Gehl “Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network” (2016) *New media & society* 2016, Vol. 18(7) 1219–1235.

¹¹⁶ See, for example, information on Tor project, available at:

<https://www.torproject.org/about/torusers.html.en#activists> (last visited 26 April 2017).

Similar technologies are used by media. See J. Ball in *Guardian* (June 2014), available at: <https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents> (last visited April 2017).

¹¹⁷ See, for example, information on Tor project, available at:

<https://www.torproject.org/about/torusers.html.en#lawenforcement> (last visited 26 April 2017).

¹¹⁸ D. Bradbury “Unveiling the dark web” (2014); G. Owen, N. Savage “The Tor Dark Net” (2015), Centre for International Governance Innovation and the Royal Institute of International Affairs, available at: https://www.ourinternet.org/sites/default/files/publications/no20_0.pdf (last visited 20 May 2017).

¹¹⁹ Here, one can use the famous example of Silk Road, the black market website, operated by US citizen. See Civil Forfeiture complaint, *US vs Ross William Ulbricht*, received 30 Sept 2013. Available at: www.scribd.com/doc/172993645/Civil-Forfeiture-Complaint (last visited 26 April 2017) cited by D. Bradbury in “Unveiling the dark web”.

¹²⁰ J. Falconer, *Mail-Order Drugs, Hitmen & Child Porn: A Journey into the Dark Corners of the Deep Web*, *Next Web* (Oct. 8, 2012, 2:56 AM), available at: <http://thenextweb.com/insider/2012/10/08/mail-order-drugs-hitmen-child-porn-a-journey-into-the-dark-corners-of-the-deep-web/> (last visited 27 April 2017) cited by A. Haasz, “Underneath It All: Policing International Child Pornography on the Dark Web”.

¹²¹ G. Owen, N. Savage “The Tor Dark Net” (2015).

¹²² The authors noted, though, that due to the anonymity offered by Tor, it is not possible to link two separate requests to the same person, but since their computer will remember descriptors until the Tor software is restarted, it often will not make multiple requests within a 24-hour period. Thus, it is logical to assume that most of this requests had been made by individual users.

number still demonstrates at least a trend in relation to number viewing child sexual abuse materials, that remains of importance for the purposes of this thesis.

Naturally, Tor is not the only technological tool used for such purposes.¹²³ ICT is a constantly evolving and fast-adapting field, often motivated by the ideas of freedom of the Internet, and still abused by those interested in illicit activities. Every step forward made by the governments and law enforcement agencies is met with yet another development, allowing darknet users to escape prosecution.¹²⁴

It is, however, important to keep in mind that it is still possible to detect, investigate and prosecute offences committed on the darknet. The anonymity protection of Tor is not absolute. As it was noticed by Meghan Neal, while the IP addresses of sites on the Tor network are concealed, they have a digital fingerprint that can be used to identify services hosted from a single location, and track visits to that site.¹²⁵ It is true, that the webpages on the darknet are constantly changing their IP addresses, at least to the eyes of outside observer, but some things can still be traced, thus allowing the police forces to investigate crimes. Moreover, as it has been noted by the director of the Tor project, it is possible to monitor the activities of Tor users before and after they reach the dark web with the help of major Internet Service Providers (ISPs).¹²⁶ That, in turn, raises another question - how far the collaboration between state agencies and ISPs can and should go before it violates the right to private life, guaranteed for any individual by major human rights instruments? Such broad control can easily turn into the weapon of mass surveillance in hands of a semi-democratic government. The issue, thus, remains of concern for the public, and is examined more closely in the next sections.

¹²³ Another example might be the Invisible Internet Project (I2P) which is also used to protect anonymity. More information available at the project's website - <https://geti2p.net/en/> (last visited 27 April 2017).

¹²⁴ One example would be to cite D. Bradbury: "*Aaron Johnson, who works The US Naval Research Laboratory, suggests that traffic analysis could help to strip the anonymity from Tor. By correlating patterns in clear-text traffic entering and leaving the network, they may be able to infer information about that traffic, along with the senders and receivers.*

This has led to proposals for dark web protocols that are resistant to traffic analysis and correlation. One, called Aqua, uses traffic obfuscation techniques, further developing on a long-discussed concept of introducing latency and decoy traffic to throw snoopers off the scent" in D. Bradbury "Unveiling the dark web".

¹²⁵ M. Neal "To Bust a Giant Porn Ring, Did the FBI Crack the Dark Web?", Vice (September 2013), available at:

<http://motherboard.vice.com/blog/the-fbi-says-it-busted-the-biggest-child-porn-ring-on-the-deep-web-1> (last visited 27 April 2017).

¹²⁶ D. Bradbury "Unveiling the dark web"; G. Owen, N. Savage "The Tor Dark Net" (2015).

3.3 Fears and Concerns In Regards to Investigations on the Internet

As it was pointed out by Owen and Savage, the means used by governments to monitor individuals' activities on the Internet allows them to track millions of letters sent with the use of anonymising software without revealing themselves.¹²⁷ The authors link their conclusions to the leaks from Edward Snowden claiming that mass surveillance can indeed be performed, and is performed by some states. One of the most commonly used justifications for this is quite ironically the complexity of the ICT. Since technologies evolve so quickly, and protection of the private data becomes more advanced, crime investigation meet with the growing numbers of barriers which are quite difficult to overcome. There is a need of modern equipment, finances, as well as for human resources capable to work with these technological means. Such lack of protection and control have been seen by David Cameron and James Comey as a threat to state security.¹²⁸

Moreover, it had been confirmed by International Association of Chiefs of Police (IACP) and EUROPOL that the use of hacking technologies brings significant investigative benefits¹²⁹, as it sometimes not possible to investigate a crime without it.¹³⁰ There is a growing trend among the states to allow broader use of hacking technologies¹³¹ during the state of emergency, as

¹²⁷ G. Owen, N. Savage "The Tor Dark Net" (2015).

¹²⁸ As it is mentioned by Abelson, H. et al. in "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications" cited by Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices", study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee (2017), available at: <http://www.europarl.europa.eu/supporting-analyses> (last visited 28 April 2017). See also, Walker, 2015, citing some Russian parliamentary opinions on the Internet undermining the idea of sovereignty, available at: <https://www.theguardian.com/world/2015/sep/01/russia-internet-privacy-laws-control-web> (last visited 28 April 2017).

¹²⁹ "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices", study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee (2017), available at: <http://www.europarl.europa.eu/supporting-analyses> (last visited 28 April 2017).

¹³⁰ IACP Summit Report, "Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence" (2015).

¹³¹ Here, as it explained by authors of the study, hacking technologies mean exploiting any possible vulnerabilities – including technical, system and/or human vulnerabilities – within an information technology (IT) system.

well as for the reasons of preventing terrorism and other crimes. These technologies are also being used in so-called “grey” areas, i.e. in absence of regulations on the matter.¹³² The situation is not differ much on the global context, with the states sometimes trying to cover the investigating activities on the Internet. That certainly raises a concern among the public and international actors¹³³ on human rights field as it is widely known how easily such broad powers can be abused by semi-democratic or nondemocratic regimes. Thus, as it was noted by Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, states increasingly require ISP’s to comply with censorship demands.¹³⁴ In accordance to the Report, surveillance presents a disproportionate impact on the freedom of expression, may raise fears and concerns among the ordinary citizens as well as undermine security online and access to information and ideas.¹³⁵

It is worth mentioning that hacking technologies reveal much more personal data than the means used to track the activities on the darknet. It is possible to make certain conclusions by monitoring accesses to the darknet, however, by the use of hacking technologies one can gain an access to all the data stored by user on their personal computer, which presents to be extremely sensitive. Not only such means allow one to see that two or more users are communicating, but the content of conversations. While these technologies can be of a great help in revealing paedophiles operating on the darknet, it is impossible to neglect the risk they bring.

The risks have also been acknowledged by the European Union Agency for Network and Information Security (ENISA) and EUROPOL in their Joint statement in 2016¹³⁶, and there are certain limitations to use of hacking technologies in crime investigation and prevention processes. Thus, for example, in some countries there is a list of crimes for which such

¹³² “Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices” (2017).

¹³³ Including UN General Assembly that noted that the development of ICT *enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern.* “The right to privacy in the digital age” (2016), A/C.3/71/L.39/Rev.1.

¹³⁴ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (2016), A/HRC/32/38.

¹³⁵ *Ibid.*

¹³⁶ “On lawful criminal investigation that respects the 21st Century data protection”. EUROPOL and ENISA Joint Statement (2016).

measures are permitted. There are also restrictions on duration of the use of technologies, although they vary from state to state and can be extended under specific circumstances.¹³⁷

¹³⁷ “Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices” (2017).

3.4 Limitations Posed by Right to Private Life and Freedom of Expression

3.4.1 Right to Private Life and Freedom of Expression

As it was mentioned on the previous subchapters, rights to private life and freedom of expression had traditionally been used as a counterpose to the need to protect the rights of children.

The right to private life also remains one of the cornerstones of modern legal regime, secured in the legal instruments on different levels, including Article 12 UDHR, Article 17 ICCPR, Article 8 ECHR, Article 5 OAS Declaration of the Rights and Duties of Man, Article 7 EU Charter of Fundamental Rights and domestic constitutions. States are therefore obliged to take active steps to protect rights of their citizens from abuses which may come on different levels, including the State itself. ECtHR has repeatedly found States responsible for the situations occurred on the Internet, including those related to private and family life,¹³⁸ protection of personal data and freedom of expression and a free flow of information.¹³⁹ Protection of the personal data is also covered by the protection of the right to private life in European context.¹⁴⁰ It would not be exaggeration to claim that in the meantime, the cyberspace and technologies is indeed the subject of surveillance of many different kinds, which had been condemned on some points by the European Court as the practices do not fulfil the criteria of proportionality under the Article 8 of the ECHR.¹⁴¹ Freedom of expression and the right to free speech are also presented as one of the most important rights of a human being often viewed as an essential for the workings of democracy.¹⁴² It is protected by various international legal instruments, such as, for example, Article 19 UDHR, Article 19 ICCPR, Article 13 of Article 10 of the ECHR, Article 13 of ACHR, Article 19 of African Charter on

¹³⁸ See, for example, K.U. v. Finland, application no. 2872/02.

¹³⁹ See, for example, Cengiz and Others v. Turkey, applications nos. 48226/10 and 14027/11.

¹⁴⁰ See, M.S. v. Sweden judgment the European Court of Human Rights, as the Court stated that “*the protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8*” (of ECHR), application no. 20837/92.

¹⁴¹ See, for example, Copland v. the United Kingdom, application no. 62617/00.

¹⁴² See, for example, Handyside v. the United Kingdom, application no. 5493/72.

Human and Peoples' Rights. On a national levels one of the most prominent examples would be First Amendment of the US Constitution.

As the question of the balance between rights is the one that is often raised in regards to means and methods used during investigation process, it would be wise to mention that both right to private life and freedom of expression are not absolute, and can be restricted under specified circumstances as long as the state's interference is in accordance with the law, passes the necessity and proportionality assessment, and pursues a legitimate aims, among which the prevention of disorder or crime and protection of the rights and freedoms of others are mentioned. Indeed, the attempts had been made to regulate the notion of balance. Thus, as it stated in EU Directive 2011/92/EU, child pornography, which constitutes child sexual abuse images, is a specific type of content which cannot be construed as the expression of an opinion.¹⁴³ Same has been noted by the US Supreme Court in *Ferber v. New York* where the Court pointed out that the notion of child pornography is not covered under the freedom of speech.¹⁴⁴ Still, the balance of rights can be, and is used as a tool to escape prosecution as it is illustrated by recent US case-law.¹⁴⁵

3.4.2 The US example

Thus, in *United States v. Michaud* the government was obliged to reveal the network investigative technique (NIT) which they used to overcome the Tor protection and uncover paedophile ring operated in the darknet. When the Department of Justice refused to do so for the sake of national security protection, the evidences obtained through the use of NIT were ordered to be excluded.¹⁴⁶ In another case, *United States v. Walter E. Ackerman*, the Internet service provider had a automated filter designed to thwart the transmission of child pornography, which marked a several images in Mr. Ackerman's emails. ISP then forwarded the materials to National Center for Missing and Exploited Children (NCMEC), the entity which gets funding from the government. NCMEC opened the email without a warrant and

¹⁴³ Preamble to the EU Directive on combating the sexual abuse and sexual exploitation of children and child pornography 2011/92/EU (2011), para 46.

¹⁴⁴ P.I. *Ferber v. New York* (1982).

¹⁴⁵ *United States v. Michaud* (2016); *United States v. Walter E. Ackerman*, appeal (2016).

¹⁴⁶ See, C. Farivar "Once more, a judge rules against gov't in Tor-enabled child porn case" (2016), available at: <https://arstechnica.com/tech-policy/2016/05/once-more-a-judge-rules-against-govt-in-tor-enabled-child-porn-case/> (last visited 12 May 2017).

discovered that these were indeed child sexual abuse materials. The materials were used as an evidence in against Mr. Akerman, who challenged the lawfulness of the performed search and won the debate as the evidences were marked as *fruits of a poisonous tree* and suppressed.¹⁴⁷

These examples illustrate how simple it can be for paedophiles operating on the darknet, to challenge the legitimacy of evidences, gained with the use of ICT. Without underestimating the risk posed by wide use of surveillance techniques by law enforcement agencies for the democratic society, one still needs to take into account the rights of victims and the need to prevent such a grave violations of children's rights as crimes of child pornography. It presents to be relatively hard to obtain an information that will allow law enforcement agency to identify the offender without the use of means amounted to surveillance or hacking techniques. Thus, the balance often shifts from the rights of victims of child sexual exploitation.

3.4.3 *The EU approach on data protection*

In 2014 the Data Retention Directive (Directive 2006/24)¹⁴⁸ that obliged states to store user data for the period of from six months to two years, was found invalid¹⁴⁹ as it violated right to respect for private life and protection of personal data of individuals secured in the EU Charter of Fundamental Rights.¹⁵⁰ Not only the Directive was found invalid by the CJEU, but also national laws that implemented it are considered by the CJEU to be in breach of the rights of individuals. The Court confirmed its position in the end of 2016 in Tele2 Sverige judgement.¹⁵¹ Here, the Court specified that the laws that oblige service providers to indiscriminately retain all the data of subscribers and users, correspond to the data retention under the Directive 2006/24,¹⁵² such a broad interference with the rights of individuals presumed to be unproportional and unjustified in a democratic society.¹⁵³ Provisions of EU

¹⁴⁷ Tenth Circuit's decision in U.S. v. Ackerman (2016), available at: <https://www.gpo.gov/fdsys/pkg/USCOURTS-ca10-14-03265/pdf/USCOURTS-ca10-14-03265-0.pdf> (last visited 12 May 2017).

¹⁴⁸ Directive 2006/24/EC.

¹⁴⁹ Judgment of the CJEU (Grand Chamber) of 8 April 2014, joined cases C-293/12 and C-594/12.

¹⁵⁰ Articles 7 and 8 of the EU Charter of Fundamental Rights.

¹⁵¹ Judgment of the CJEU (Grand Chamber) of 21 December 2016, joined cases C-203/15 and C-698/15.

¹⁵² Judgment of the CJEU (Grand Chamber) of 21 December 2016, joined cases C-203/15 and C-698/15, para 97.

¹⁵³ Judgment of the CJEU (Grand Chamber) of 21 December 2016, joined cases C-203/15 and C-698/15, paras 100-112.

Charter of Fundamental rights thus override national laws that allow “*general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication*”.¹⁵⁴

That said, the Article 15(1) of Directive 2002/58, that was amended by Directive 2006/24, provides four exemptions under which it is possible to restrict the rights, namely, “*to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system*”.¹⁵⁵ The interference still must be necessary in a democratic society, appropriate and proportionate. The Court confirmed this rule in its *Tele2 Sverige* judgement, specifically pointing out that “*since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data*”.¹⁵⁶ The question is, however, if crimes of viewing child sexual abuse or exploitation materials on the Internet can be considered as a serious enough to justify the access to such a broad data, and if not, should they at least partly be included under the said provision? That question remains largely unanswered on a global scale. Here, case-law of the ECtHR can be used as an example of a positive practice to address such balance.

3.4.4 The ECtHR approach

The stance taken by the ECtHR in relation to child sexual abuse materials is quite opposite to those of EU and US. The first case related to child sexual abuse materials examined by ECtHR was *Karttunen v. Finland*¹⁵⁷. This case concerned the applicant that downloaded hundreds of images of child sexual abuse and exploitation and were intended to make an exhibition of it for the purposes to illustrate the ease of the access to material and engage a public discussion on the problem. The exhibition, however, was closed, and the applicant

¹⁵⁴ Judgment of the CJEU (Grand Chamber) of 21 December 2016, joined cases C-203/15 and C-698/15, para 112.

¹⁵⁵ Article 15(1) of Directive 2002/58.

¹⁵⁶ Judgment of the CJEU (Grand Chamber) of 21 December 2016, joined cases C-203/15 and C-698/15, para 115.

¹⁵⁷ *Karttunen v. Finland*, 2011, application no. 2872/02.

convicted of possession and distribution of sexually obscene pictures depicting minors.¹⁵⁸ The ECtHR stated that despite the lack of sanctions against the applicant, the conviction amounted to the interference with her right to freedom of expression, thus claiming that possession and distribution of child sexual abuse materials falls under the scope of freedom of expression.¹⁵⁹ Nevertheless, the interference was proportionate to the legitimate aim pursued as the “*the criminalisation of child pornography was based on the interests of protecting children from sexual abuse, their privacy rights, and also moral considerations*”.¹⁶⁰

The approach taken by ECtHR in *Karttunen v. Finland* illustrates the position expressed by Gillespie. Thus, in the European context criminalisation of possession of child sexual abuse materials would probably be considered as proportional to a pressing social need to protect morals given the views on child sexual abuse within the society.¹⁶¹ Same can be claimed in relation to viewing of child sexual abuse materials, as it leads to devastating consequences in child development and gravely violates children’s rights.

Here, it would be of interest to notice that in the European context it is required of states to have a system that is aimed “*to protect child victims from being exposed as targets for paedophilic approaches via the Internet*”.¹⁶² Thus, in *K.U. v. Finland*, ECtHR found the state in violation of the rights to private and family life of the applicant due to the absence of effective steps taken to identify and prosecute the perpetrator that exposed a 12 years old child to the paedophiles on the Internet.¹⁶³ The ECtHR reinforced the position that states have positive obligations under the Article 8 ECHR¹⁶⁴ and pointed out that these obligations cover criminalising offences against an individual and application of criminal law provisions in practice through effective investigation and prosecution.¹⁶⁵ Furthermore, the Court noted that “*where the physical and moral welfare of a child is threatened such injunction assumes even*

¹⁵⁸ Rónán Ó Fathaigh in Strasbourgh Observers “*Karttunen v. Finland: Child Pornography and Freedom of Expression*” (2011), available at: <https://strasbourghobservers.com/2011/10/10/child-pornography-and-freedom-of-expression/> (last visited 10 May 2017).

¹⁵⁹ *Karttunen v. Finland*, application no. 2872/02, para 17.

¹⁶⁰ Rónán Ó Fathaigh in Strasbourgh Observers “*Karttunen v. Finland: Child Pornography and Freedom of Expression*” (2011).

¹⁶¹ A. Gillespie, “*Child Pornography: Law and Policy*” (2011), p. 116.

¹⁶² *K.U. v. Finland*, application no. 2872/02, para 47.

¹⁶³ *K.U. v. Finland*, para 49.

¹⁶⁴ *K.U. v. Finland*, para 46.

¹⁶⁵ See *M.C. v. Bulgaria* para 153.

greater importance".¹⁶⁶ There are, however, no strict guidelines on the extent of such protection, that results on the differences among legislation even within the region.¹⁶⁷

Summarising, it can be claimed that despite nearly universal ratification of CRC, the protection of children's rights is still ineffective as there is no consistency among national legislations, or case-law. Thus, in a current situation, the decision on the each individual case would depend very much on the national and regional practice of the prosecuting party. Therefore, it seems relevant to analyse further the potential for the jurisdictional disputes as well as effort towards collaboration which are being made on different levels. These issues are addressed on the following subchapter.

¹⁶⁶ K.U. v. Finland, para 46.

¹⁶⁷ Thus, for example, viewing child sexual abuse materials is a crime in Sweden, but not in Russia, though both countries ratified CRC, OPSC and Lanzarote Convention among other instruments. Sources - Criminal Codes of both countries read by the author of this paper.

3.5 Jurisdictional Disputes and International Cooperation

As it was mentioned before, the major differences in legislation start already with the notion of child, and then only broaden to the question of what materials are considered to be child pornography, and what actions regarding to these materials are criminalised. However, that is only a part of the problem. Another issue rises from the procedural perspective as powers of the law enforcement agencies, standards of gathering of evidences or court proceedings differ from country to country. Thus, obtaining evidences from ISP's that operate in a different country, present to be rather difficult, expensive and time-consuming process.¹⁶⁸ Moreover, the very nature of the Internet makes it possible that the law enforcement unit of one state might accidentally hack into the computer, located on the territory of another.¹⁶⁹

3.5.1 Jurisdiction

Jurisdictional disputes present to be a known and inevitable trait of the offences related to the Internet. Problems, however, change with the type of jurisdiction applied in every different case. Thus, under the notion of the territorial jurisdiction, one can come up with the situation when several states have jurisdiction over the crime since it was committed on their territory. Referring to the example used in the epigraph to the current chapter, A. Haasz notes that Barbados, St. Lucia, Italy, and the U.S. can all have jurisdiction under territorial jurisdiction in this case.¹⁷⁰ With the use of extraterritorial jurisdiction, states can still prosecute their nationals that are viewing child sexual abuse and exploitation materials while being on the territory of the country which does not have laws against this type of a crime.¹⁷¹ Thus, Australia would also have jurisdiction over those committing abuse; and also any other state that is criminalises viewing child sexual abuse materials over nationals that viewed the video

¹⁶⁸ Global Alliance Against Child Sexual Abuse Online “2015 Threat Assessment Report” (2015).

¹⁶⁹ Such disputes can be found even within one country. Thus, in *United States v. Michaud* (2016) mentioned earlier, the fact that NIT-warrant was issued by the court of one state to obtain information from the computer located in another state, was also disputed during the proceedings.

¹⁷⁰ A. Haasz, “Underneath It All: Policing International Child Pornography on the Dark Web” (2016).

¹⁷¹ *Ibid.*

on the dark web, if they apply a protective principle.¹⁷² Hence, there are a few competing jurisdictions in that case, as there are in almost any other case of viewing child sexual abuse or exploitation materials on the Internet.

One can say, it is difficult to define which particular jurisdiction should take over in each case, as there cannot be strict guidelines for every type of different jurisdictional conflict between different states in such situations. Moreover, as Haasz points out, it is known to crimes go uninvestigated because it is impossible to define the jurisdiction if the location of images is unknown.¹⁷³ There are, however, certain mechanisms to regulate these problems as states are indeed required to provide mutual assistance in crime investigation and extradition by the international instruments.¹⁷⁴ The most obvious example would be a bilateral or multilateral treaty. OPSC, EU Directive and Council of Europe Conventions set some criteria for such situations.¹⁷⁵ Thus, OPSC encouraged states to apply rules of extraterritorial jurisdiction to prosecute those who committed offenses of child sexual exploitation and abuse outside national territory.¹⁷⁶

3.5.2 Cooperation

Cooperation is viewed to be the key factor in resolving jurisdictional disputes. As it is stated in the para 49 of the Preamble to EU Directive on combating the sexual abuse and sexual exploitation of children and child pornography, states cannot effectively investigate and prevent crimes of that type alone, therefore the objectives considered to be better achieved at the Union level. States are also encouraged to collaborate with the non-member states in relation to block the access to child sexual abuse or exploitation materials, or take down web pages with such content.

Important achievements can be seen in work of INTERPOL and EUROPOL as they are aimed for the collaboration between law enforcement agencies of different countries. Thus, in

¹⁷² A. Haasz, “Underneath It All: Policing International Child Pornography on the Dark Web” (2016).

¹⁷³ *Ibid.*

¹⁷⁴ See, for example, Articles 6, 7, 10 OPSC, Article 34 CRC, and some other programme documents, for example, United Nations “A World Fit for Children” (UN Doc. GA/RES/S-27/2, 2002).

¹⁷⁵ Thus, for example, the Article 25(8) of Lanzarote Convention states that “*when more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution*”.

¹⁷⁶ Article 4 OPSC.

2011 INTERPOL General Assembly issued a recommendation to make the expertise of General Secretariat available in supporting the National Center Bureaus and parties involved in creating appropriate legal tools to combating online sexual exploitation of children¹⁷⁷ as some countries do not have sufficient policies on the matter. Earlier, in 2009, INTERPOL General Assembly encouraged states “*to promote the use of all the technical tools available, including access-blocking of websites containing child sexual abuse images, in order to intensify the fight by their national specialized units against the dissemination of child sexual abuse images on the Internet*”.¹⁷⁸ INTERPOL’s International Child Sexual Exploitation (ICSE) database is one of the most prominent examples of such tools. ICSE database provides law enforcement agencies with the special software that analyses the content of the materials and helps to make connections between images of victims, abusers and locations. As it is claimed on INTERPOL’s website, ICSE database helps to identify on average five victims per day.¹⁷⁹ Problems might arise during this process, if materials had been modified to some extent, as Haasz points out.¹⁸⁰ That, however, can be dealt with by introducing more advanced technologies. Still, as it was said earlier law enforcement agencies are generally in need of more officers trained to work with ICT to overcome such problems.

There are other technological cooperations, most known would be COSPOL Internet Related Child Abusive Material Project (CIRCAMP), a network founded by the European Commission, that is aimed to collaborate with ISP’s to filter and block the access to web resources which contain child sexual abuse materials.¹⁸¹ Both EUROPOL and INTERPOL are part of the project, the latter is also running its own “Worst of”-list in necessity of a global initiative.¹⁸² Filtering technologies are working on the national levels, thus, for example, in Sweden when attempting to enter blocked website, the “stop-page” opens that explains that

¹⁷⁷ INTERPOL GA Resolution “Combating online sexual exploitation of children through a legislative global engagement strategy”, (2011), AG-2011-RES-05.

¹⁷⁸ INTERPOL GA Resolution “Combating sexual exploitation of children on the Internet using all available technical solutions, including access-blocking by INTERPOL member countries”, (2009), AG-2009-RES-05.

¹⁷⁹ INTERPOL “Global operation targets child sexual abuse material exchanged via messaging apps” (2017), available at: <https://www.interpol.int/News-and-media/News/2017/N2017-047> (last visited 12 May 2017).

¹⁸⁰ A. Haasz, “Underneath It All: Policing International Child Pornography on the Dark Web” (2016).

¹⁸¹ M. Eneman, “Access Blocking of Child Abusive Material: Evaluation of the Swedish Practice” (2012), Conference Proceedings of the 4th International Symposium on Children at Risk and in Need of Protection, available at:

<https://gup.uu.se/publication/156041> (last visited 12 May 2017).

¹⁸² INTERPOL “Crimes Against Children, Access blocking”. Available at:

<https://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking> (last visited 12 May 2017).

content of that particular resource is illegal, and explains how one can complain against blocked domains. The collaboration between police and Swedish ISP's, as Eneman points out, is voluntary, and had received some criticism for being a censorship of a kind.¹⁸³ It is equally free of charge and voluntary to take part in INTERPOL's "Worst of"-list.¹⁸⁴

Actions are also taken to target crimes committed with use of new technologies. One of the recent examples being an Operation Tantalio, which was launched in 2016 by Spanish police in cooperation with law enforcement agencies in 15 other countries in Latin America and Europe,¹⁸⁵ and coordinated by INTERPOL and EUROPOL. During the operation hundreds of images of child sexual abuse were discovered, and individuals that used the messaging application WhatsApp to exchange child sexual abuse and exploitation materials, were targeted and arrested.¹⁸⁶

Another problem lies in the resources and tools available for the police, existence of special units or officers getting a training to work with ICT, opportunities to cooperate with ISPs and Internet companies, as well as interstate cooperation. These issues are examined in the next chapter alongside with the need for a new legislation or guidelines and other potential solutions.

¹⁸³ M. Eneman, "Access Blocking of Child Abusive Material: Evaluation of the Swedish Practice" (2012).

¹⁸⁴ INTERPOL "Crimes Against Children, Access blocking".

¹⁸⁵ Countries participating in the operation are Argentina, Bolivia, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Germany, Guatemala, Italy, Mexico, Paraguay, Peru, Portugal and Spain. INTERPOL "Global operation targets child sexual abuse material exchanged via messaging apps" (2017), available at: <https://www.interpol.int/News-and-media/News/2017/N2017-047> (last visited 12 May 2017).

¹⁸⁶ INTERPOL "Global operation targets child sexual abuse material exchanged via messaging apps" (2017).

4 Chapter Four: Combating Viewing Child Sexual Abuse Materials on the Internet

4.1 Call For Action

Summarising previous chapters, it cannot be said that the crime of viewing child sexual abuse materials completely falls out of the attention of international community. Calls for criminalising such offences had been made in international society for more than a decade now, however, there had not been enough actions taken. At the same time the situation on the ground makes it difficult to investigate these crimes. There are still large differences among national legislations as well as jurisdictional disputes arising due to the global nature of the crime. Case-law on the matter is also inconsistent, allowing offenders to escape prosecution due to the technicalities. Still, it is evident that viewing child sexual abuse materials on the Internet further infringes the rights of the child that is being abused and(or) exploited for the production of materials. Thus, the action must be taken, preferably on different levels, including not only lawmaking process, but advocacy and educative means, as there is a persistent need of more qualified approach take by both law enforcement agencies and civil society.

In a light of inconsistency and weakness of existing national legislation, it seems logical to start by determining grounds for states' obligations to protect children's rights by criminalising viewing child sexual abuse materials. The chapter then proceeds to the potential of creating a new treaty, a call for which had been expressed multiple times during past decades.¹⁸⁷ In the following subchapter I also take notice on the need to more broad cooperation between law enforcement agencies and ISPs. Potential of broader collaboration among law enforcement agencies on the matter is also taken into the account. The next subchapter addresses actions taken by the Internet corporations such as Google and

¹⁸⁷ J. Carr, Z. Hilton in "Internet Child Abuse. Current Research and Policy" edited by J. Davidson and P. Gottschalk (2011), p. 58.

Microsoft, role of corporate social responsibility (CSR) in regards to crime prevention and investigation. Civil society and NGOs are also playing an important part in the process of education in all sectors and spreading awareness on the issue, thus it seems wise to mention them on a final part of the chapter before proceeding to the concluding remarks.

As the problem of viewing child sexual abuse materials on the Internet presents to be a rather complicated one with a lot of aggravating factors affecting both the violations of children's rights and investigation process, the list of solutions mentioned in the current chapter is not an exhaustive. There are other means and methods that can and should be used to combat the crime of viewing child sexual abuse or exploitation materials on the Internet. Thus, as it falls out of the scope of this thesis to analyse all the potential solutions, I've chosen to focus on those that hold the most of potential in a contemporary situation.

It is important to note that all of suggested solutions are aimed to collaboration, first and foremost, on an international level, as such widespread global crime aggravated by constantly evolving ICT can only be effectively combated by a concerted action. That said, an action taken internationally would fail without a proper base in a national legislation. Thus, there is a simultaneous need for harmonisation of national legislation on the notion of viewing child sexual abuse and exploitation materials on the Internet.¹⁸⁸

¹⁸⁸ ICMEC "Child Pornography: Model Legislation & Global Review" International Centre for Missing & Exploited Children (ICMEC) (2016).

4.2 Obligations to Criminalise Viewing Child Sexual Abuse and Exploitation Materials on the Internet

It seems important to claim that children do have the right to protection from all forms of violence under the scope of CRC. As it was mentioned before, the CRC had been almost universally recognised. There are 196 parties to the Convention as of April 2017, and 173 parties to the OPSC. Due to such wide ratification, some scholars claimed that at least some provisions of the CRC have a status of *jus cogens*.¹⁸⁹ Van Bueren argues, that some forms of child sexual exploitation amount to slavery practices. Another example would be the prohibition of torture or other cruel, inhuman or degrading treatment, secured in the Article 37 of the Convention. In its General Comment No. 8 the Committee on the Rights of the Child specified that the provisions of Article 37 are complemented and extended by the Article 19, that obliges states to take all appropriate measures to protect children from all forms of physical or mental violence, injuries, abuses and exploitation, including sexual abuse. Moreover, Article 34 specifically requires states to protect the child from all forms of sexual exploitation and sexual abuse. As it was stated before, child pornography is in itself an evidence of child sexual abuse and exploitation, moreover it can (and often does) lead to a mental traumas as well, since materials are constantly reproduced with the use of ICT. Not only CRC protects children in this manner. Article 10(3) of ICESCR also obliges states to make employment of children in work harmful to their morals or health punishable by law. Such type of work cover different forms of sexual exploitation including the use of children in pornography. The use of children in pornography is also included into the notion of the worst form of child labour provided by ILO Convention on the Worst Form of Child Labour.¹⁹⁰ Hence, it can be claimed that states have an obligation to protect all the children under their jurisdiction from all forms of sexual abuse, including child pornography, though not all means and methods can be used without raising a concern in regards of potential violations of other rights.

¹⁸⁹ See, for example, G. Van Bueren in “The International Law on the Rights of the Child” (1998).

¹⁹⁰ ILO Convention No. 182, Article 3(b).

Remarkably, despite such requirement, the OPSC remains the only universal treaty specifically addressing the issue of child pornography,¹⁹¹ with some reservations rising a significant amount of doubt to states' commitment to welfare protection.¹⁹² There are, however, certain regional developments such as Convention on Cybercrime or Lanzarote Convention. Thus, for example, Article 20(f) of the Lanzarote Convention requires states to criminalise knowingly obtaining access to child pornography through ICT. As it is seen from the Explanatory Report to the Convention, this element is added specifically to catch those who cannot therefore be caught under the offence of procuring or possession in some jurisdictions. Yet, there are some reservations to the Convention which are worth mentioning as an illustration to inconsistency of legislations on the matter among the states even though they are parties to the same treaties. Thus, for example, Belgium, Bulgaria, Luxembourg and Russia among others have reserved the right not to criminalise offences established in accordance with Article 20, paragraph 1(f), namely possessing child pornography and knowingly obtaining access, through information and communication technologies, to child pornography.¹⁹³ France and Germany have reserved the right not to criminalise attempts to knowingly obtain access to child sexual abuse materials with the use of ICT.¹⁹⁴

Yet such developments can be seen as opposing the provisions of CRC as states must take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of violence and abuses under the Article 19 of thereof. The underlying problem, however, is that there are no working mechanisms to ensure compliance with the CRC, as it was pointed out by Carr and Hilton.¹⁹⁵

It seems fair to point out that attempts to cover gaps between national legislations had been made. In its 2015 Report Global Alliance Against Child Sexual Abuse Online noted that at

¹⁹¹ J. Carr, Z. Hilton in "Internet Child Abuse. Current Research and Policy" edited by J. Davidson and P. Gottschalk (2011), p. 55.

¹⁹² E. Quayle, L. Loof, T. Palmer "Child Pornography and Sexual Exploitation of Children Online" (2008) cited by J. Carr, Z. Hilton in "Internet Child Abuse. Current Research and Policy" edited by J. Davidson and P. Gottschalk (2011), p. 56.

¹⁹³ Reservations and Declarations to Lanzarote Convention, available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/declarations?p_auth=Dcse9AWV (last visited 17 May 2017).

¹⁹⁴ *Ibid.*

¹⁹⁵ J. Carr, Z. Hilton in "Internet Child Abuse. Current Research and Policy" edited by J. Davidson and P. Gottschalk (2011), p. 56.

least some states are in the process of amending laws to close lacoons previously used by perpetrators.¹⁹⁶

Still, it is of importance not only to adopt a legislation criminalising viewing child sexual abuse and exploitation materials on the Internet, but educate both law enforcement sector and business on the importance of a proper functioning of such legislation. Hence, there is a need of more effective regulative mechanisms and collaboration tools, as well as raising awareness on the matter and legislation among the public and ISPs, which are analysed in coming subchapters.

¹⁹⁶ Global Alliance Against Child Sexual Abuse Online “2015 Report” (2015), available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_2015_report_en.pdf (last visited 22 May 2017).

4.3 A Need For a New Treaty v. the Use of Existing Instruments

4.3.1. A New Instrument

As it was pointed out in previous subchapter, despite all the obligations imposed on states by international legal instruments, laws remains inconsistent thus providing loopholes for offenders that view child sexual abuse or exploitation materials on the Internet. States are reluctant to fully implement existing treaties, which, in turn, also differ in both terms of terminology and the scope of protection. As Haasz points out there is no requirement to ratify a treaty that prohibits child pornography,¹⁹⁷ it is also possible to make a reservations on the provisions related to the implementation of the treaty to national legislation in relation to child sexual abuse crimes. In absence of clear regulations, there is always risk that the offence would fall out the protection as it is clearly happening on practice. Problems starting with the notion of a child, consent, sexual abuse and means used for production and distribution of materials. To the point of investigation, prosecution and crime prevention, differences among national legislations become so broad, that it is hardly possible for law enforcement agencies to legally fulfil their responsibilities, unless the operation is coordinated by INTERPOL or EUROPOL.

Technology is a double-edged sword. There are certain mechanisms that allows law enforcement agencies to determine trends in usage of anonymising tools, thus to discover activities which may potentially be related to viewing child sexual exploitation materials. The flow of funds can be named as one of the examples of such means, sometimes being the only link between viewer and distributor or perpetrator.¹⁹⁸ However, it is difficult to get an access to the exact nature of the materials viewed by user on the darknet without the use of hacking techniques, thus potentially being in a breach of fundamental rights of an individual. Although such means and methods are widely being used by police and states agencies, it is still gives a rise for a balance of rights questions, that, as it was illustrated by some examples

¹⁹⁷ A. Haasz, "Underneath It All: Policing International Child Pornography on the Dark Web" (2016).

¹⁹⁸ ECPAT International "Online Child Sexual Abuse and Exploitation. An Analysis of Emerging and Selected Issues" (2017), available at: http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf (last visited 20 May 2017).

in previous chapters, can result in ineffectiveness of prosecution or leave the case unprosecuted. Therefore it appears¹⁹⁹ that existing instruments cannot properly function as there are no control mechanisms, lots of reservations which are cutting down the list of punishable offences, and a constant battle between the rights. One of the reasons behind it, as it was pointed out by Carr and Hilton, can be a lack of international political action that will effectively cover all the relevant issues.²⁰⁰

Hence, it can be claimed that there is a need for a new instrument which will take into account criticism received by existing legal instruments on problem of the balance of rights, severity of the offences of child sexual exploitation and abuse materials, as well as specific nature of constantly evolving technology. Examples of such developments can be video games and live streaming, the latter being described by ECPAT International as particularly hazardous and offensive, that is difficult to address due to the absence of an adequate legal framework on viewing of child sexual abuse or exploitation materials²⁰¹. Another important development might be the notion of state responsibility. There have been examples of states being held responsible for violation of human rights for omission or not providing a sufficient protection to children.²⁰² Thus of an effectively functioning report mechanism under the major instruments on the field may be considered as a potential solution as well. New instrument should also take into account the notion of intersectionality, as it is seen from different reports and practice that the crime of child sexual exploitation is affected by the notion of poverty, social norms justifying the abuses, technological impacts and other factors.²⁰³

4.3.2 The sufficiency of existing legislation

The idea of a new instrument, however, can be opposed with the argument of sufficiency of existing legislation that provides an appropriate amount of tools for states to use in the process of investigating, prosecuting and preventing the crimes. CRC is a universally ratified

¹⁹⁹ J. Carr, Z. Hilton in “Internet Child Abuse. Current Research and Policy” edited by J. Davidson and P. Gottschalk (2011), p. 58.

²⁰⁰ *Ibid.*

²⁰¹ ECPAT International “Online Child Sexual Abuse and Exploitation. An Analysis of Emerging and Selected Issues” (2017).

²⁰² ECtHR case-law is one of those with some of the examples being *K.U. v. Finland* previously addressed in this theses, *Söderman v. Sweden*, *X and Y v. the Netherlands*, *M.C. v. Bulgaria*.

²⁰³ See, for example ECPAT International “Online Child Sexual Abuse and Exploitation. An Analysis of Emerging and Selected Issues” (2017).

instrument that imposes obligations to almost every state on the planet to protect children, there are also regional instruments that provide some definitions and resolve some of the problems. There are means and methods that are being used by police in their joint effort to combat such offences. Previously mentioned Operation Tantalio that uncovered paedophiles using WhatsApp to exchange materials, can be used as an illustration of such successful collaborations. It is also possible to claim that the process of conducting a new treaty can be rather time-consuming, with a heavy political impact, while ICT is a rather fluent, rapidly developing field, hence the law might always be behind the technological progress if one is aimed to cover all the means and methods used by offenders rather than concentrate upon the nature of offence.

Here, one should address ICMEC report on existing legislation on child sexual abuse materials “Child Pornography: model legislation & global review”, the latest edition being published in 2016, as it demonstrates trends in progress made by states towards combating child pornography.²⁰⁴ Thus, it points out that due to successful collaboration in fighting commercial trade of child sexual abuse and exploitation materials online, it had been significantly reduced over the past decade.²⁰⁵ That, however, was “compensated” by the growth of non-commercial, peer-to-peer exchange of materials, that remains largely out of the reach of law enforcement agencies. There is a persistent need for strong legislation on child sexual abuse materials in every country to combat that problem, as it is pointed out in ICMEC report.²⁰⁶

As it was mentioned before, in 2016 slightly more than 25% of examined countries (50 out of 196) do not criminalise even possession of child sexual abuse materials, these include among others Argentina, Belarus, Ukraine, Cambodia, Chile, China and Russia.²⁰⁷ Remarkably 35 states still have no legislation that specifically addresses child pornography, despite being part of CRC and other international treaties on the matter. Logically, as it is noticed by Carr and

²⁰⁴ The said progress, however, had been defined as “*painfully slow: too slow*” by Carr and Hilton. See J. Carr, Z. Hilton in “Internet Child Abuse. Current Research and Policy” edited by J. Davidson and P. Gottschalk (2011), p. 59.

²⁰⁵ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime 36 (2013), at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf cited by ICMEC “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016).

²⁰⁶ ICMEC “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016).

²⁰⁷ *Ibid.*

Hilton, that opens the way for criminals who sexually exploit and abuse children, as they can use such loopholes in international cooperation and stick to the countries lacking legislation or strict enforcement.²⁰⁸

Therefore, to fulfil obligations to protect children from sexual abuse, there is a need for states to close existing loopholes with the use of means and methods that are already in place. A new international instrument is needed to cover areas that are missing or disconnecting in current legislation, starting with the notion of technology as it significantly complicates investigation, prosecution and crime prevention processes.

The new treaty might also be needed to regulate the cooperation between law enforcement and private sector, namely ISPs. It has been noted by many that ISPs possess the ability to make a valuable contribution to the investigation and crime prevention processes. It can be also said that many of ISPs are actively cooperating with the law enforcement agencies. However, there are situations in which ISPs are actively opposing the attempts to regulate collaboration process,²⁰⁹ thus it remains voluntary in most of the states. Hence, it seems important to continue the paper by analysing the potential of such cooperation as well as obligations of ISPs.

²⁰⁸ J. Carr, Z. Hilton in “Internet Child Abuse. Current Research and Policy” edited by J. Davidson and P. Gottschalk (2011), p. 59.

²⁰⁹ The example of this would be CJEU Tele2 Sverige judgement, mentioned earlier.

4.4 Legal Regulation of the work of ISPs

Practice of collaboration with ISPs is recognised²¹⁰ to be of a high importance in order to prevent further crimes (i.e. blocking access to the sites that contain illegal materials), and investigation process (i.e. obtaining information from ISPs). It is also named as one of the essentials by ICMEC as in many cases it would be impossible to learn about child pornography offences being committed unless ISPs report it.²¹¹ ICMEC report even claims that *ISPs “are in an almost ideal position to report suspected child pornography offenses to law enforcement through content management and reports from their users”*.²¹² As it was previously noted, the very nature of the dark web, and availability of anonymising software for every user on the Internet makes it difficult for law enforcement agencies to investigate and track down individuals operating on the darknet. It is not even a requirement for a person to be particularly skilled in ICT as there are instructions on how to access and navigate the darknet published on the surface web.²¹³

It is possible, however, to perform operations, especially coordinated by such agencies as INTERPOL and EUROPOL, to take down paedophile rings or websites. There are also some legal procedures to obtain data both from ISP or the user if there is a suspicion of involvement in a serious crime. Thus, the Article 18 of the Budapest Convention requires states to adopt an appropriate legislation which will cover a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control. Similar approach is recommended by ICMEC.²¹⁴

²¹⁰ See, for example, Global Alliance Against Child Sexual Abuse Online “2015 Report”.

²¹¹ ICMEC “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016).

²¹² *Ibid.*

²¹³ Searching request “dark web access” on Google leads to 21 400 000 results, available at: <https://www.google.se/search?q=dark+web+access> (last visited 22 May 2017).

²¹⁴ ICMEC “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016).

Yet, the problems remains. As Haasz points out, despite all the technological achievements made by law enforcement agencies, it is costly and time consuming to track every individual that is accessing child sexual abuse materials on the Internet.²¹⁵ With individuals operating on the darkweb, the costs grow alongside with the demand of technological skills of the officers. Therefore, police still largely relies on a notice and takedown order that requires an ISP to block an access to particular web resources.²¹⁶ It is still possible, though, to backup servers and preserve the materials for further distribution as it happened in case of the Freedom Hosting, with over the million files with child sexual abuse and exploitation materials being backed up and made available to download with the use of torrent software.²¹⁷

Thus, it is not enough to take down a part of the dark web, nor it is enough to block an access to the web resources, as these blocks can be bypassed by skilled perpetrators with the use of TOR software. Instructions to these can also be easily found on the surface Internet. It is even advised to use such techniques to fight the state of censorship, for example, in China or in Russia.²¹⁸

Complications arise also with limits of obligations ISPs have in relation to storing and revealing user data in different countries. During the course of investigation there is a always a need for the police to follow a particular procedure to not infringe with the rights of individuals. That becomes specifically relevant in European context as with the EUCJ judgements on data retention, law enforcement agencies are only allowed to request an access to retained data solely in process of fighting serious crimes, and under special procedure such as obtaining a warrant before gaining access to the data.²¹⁹ The length of the process thus only increases.²²⁰ Taking into account further aggravations by jurisdictional disputes, in the light of rapid development of ICT that lead to offences go unprosecuted by the lack of evidences. As

²¹⁵ A. Haasz, “Underneath It All: Policing International Child Pornography on the Dark Web” (2016).

²¹⁶ *Ibid.*

²¹⁷ Patrick Howell O’Neill, An In-Depth Guide to Freedom Hosting, the Engine of the Dark Net, Daily Dot (Aug. 4, 2013) cited by A. Haasz in “Underneath It All: Policing International Child Pornography on the Dark Web” (2016).

²¹⁸ See, for example, some instructions on the access of websites blocked by Russian governmental agency on the communication, Roskomnadzor (in Russian), available at: <https://meduza.io/feature/2016/09/15/roskomnadzor-zablokiroval-moy-lyubimyy-sayt-chno-delat> (last visited 10 May 2017).

²¹⁹ Judgment of the CJEU (Grand Chamber) of 21 December 2016, joined cases C-203/15 and C-698/15, para 125.

²²⁰ ICMEC “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016)

it was noticed by International Association of Chiefs of Police cited in ICMEC report, “*the failure of the Internet access provider industry to retain subscriber information and source or destination information for any uniform, predictable, reasonable period has resulted in the absence of data, which has become a significant hindrance and even an obstacle in certain investigations*”²²¹.

That in some contexts might be viewed as a violation of the protection of the rights of children abused or exploited on the materials, since the absence of laws that oblige ISPs to reveal information that allowed to identify the offender amounts to the violation of the Article 8 ECHR.²²²

There had been debates on notion of data retention during previous years, some of them found their place in previous subchapters of this thesis. Data retention can be a powerful tool in relation to finding offenders that are using various technological tool to hide the evidences of their activities online. Thus, ICMEC expanded its research on it for the latest report taking a special notice on Canadian approach to the problem. Thus, Canada obliged ISPs to notify authorities of child pornography offenses on their network²²³ and then “*preserve all computer data related to the notification that is in their possession or control for 21 days after the day on which the notification is made*”.²²⁴ That term can be prolonged in the existence of judicial order. Although the practice are indeed of a good example, ICMEC goes further in recommendation to preserve the data “*for no less than 90 days with the possibility to request an extension*”.²²⁵ Still while there had been some developments²²⁶ on the regulation of cooperation between ISPs and law enforcement on the notifications, filtering and data retention, it mostly remains voluntarily. In a growing resistance towards the use of means and

²²¹ J. Weinstein “Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes”, Statement before the Committee on Judiciary Subcommittee on Crime, Terrorism, and Homeland Security United States House of Representatives (2011) cited by ICMEC “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016).

²²² See the position expressed by the ECtHR in *K.U. v. Finland*.

²²³ ICMEC “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016).

²²⁴ Bill C-22 respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, Sections 2 and 3 (Mar. 23, 2011) cited by ICMEC “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016).

²²⁵ ICMEC “Child Pornography: Model Legislation & Global Review” International Centre for Missing & Exploited Children (ICMEC) (2016).

²²⁶ Thus, for example, Albania’s National Agency for Computer Security (NACS) and the Authority of Electronic and Postal Communications (AEPC) signed a Memorandum of Understanding for cooperation. See Global Alliance Against Child Sexual Abuse Online “2015 Report”.

methods of mass surveillance, and ISPs opposing obligatory storing and revelation of users' personal data, there is an obvious need of more coordinated cooperation between law enforcement agencies and private sector. The task before legislators is rather difficult one, as they are required to find a proper and effective balance between the need to protect children and the need to protect private life of Internet users. Canadian approach alongside with ICMEC recommendations on good practices seems, therefore a relevant example of a potential solution.

However, it is not only ISPs that can report crimes of child pornography to law enforcement agencies. IT companies, especially those operating globally, have the opportunity to actively contribute to crime prevention. Thus, potential of such collaboration alongside with the notion of corporate social responsibility is analysed in the next subchapter.

4.5 The Potential of Corporate Social Responsibility in Combating the Offence of Viewing Child Sexual Abuse Materials on the Internet

Foundation for business sector's participation in combating child sexual abuse can be found in UN Guiding Principles on Business and Human Rights, that are often referred to as the "Ruggie principles"²²⁷ on the basis of which UNICEF, the UN Global Compact, and Save the Children developed the Children's Rights and Business Principles.²²⁸ The objective of the latter is to promote corporate responsibility to respect²²⁹ and support²³⁰ children's rights in conjunction with the government duty to protect and safeguard children's rights. The principles include, inter alia, responsibility to commit to supporting the human rights of children,²³¹ use marketing and advertisement that respect and support children's rights,²³² reinforce community and government efforts to protect and fulfil children's rights.²³³ In relation to IT sector there had been a special development with the Guidelines for Industry on Child Online Protection (COP), one of the main five aims of which being developing standard processes to handle child sexual abuse material.²³⁴ That include taking active steps to prevent companies' networks and services from being misused to disseminate child sexual abuse

²²⁷ UN HR council 'Guiding principles on business and Human Rights: Implementing the UN' "Protect, Respect and Remedy" Framework', A/HRCH/17/31 (21 March 2011) (SRSG, Guiding Principles).

²²⁸ UNICEF's children's rights and business, available at: <https://www.unicef.org/csr/47.htm> (last visited 08 May 2017).

²²⁹ That means *avoiding any infringement of human rights, including children's rights, and addressing any adverse human rights impact with which the business is involved. The corporate responsibility to respect applies to the business's own activities and to its business relationships, linked to its operations, products or services.* UNICEF's children's rights and business, available at: <https://www.unicef.org/csr/47.htm> (last visited 08 May 2017).

²³⁰ That means *in addition to respecting human rights, voluntary actions that seek to advance human rights, including children's rights, through core business activities, strategic social investment and philanthropy, advocacy and public policy engagement, working in partnership and other collective action.* UNICEF's children's rights and business, available at: <https://www.unicef.org/csr/47.htm> (last visited 08 May 2017).

²³¹ Principle 1, UNICEF's children's rights and business, available at: <https://www.unicef.org/csr/47.htm> (last visited 08 May 2017).

²³² Principle 6, UNICEF's children's rights and business, available at: <https://www.unicef.org/csr/47.htm> (last visited 08 May 2017).

²³³ Principle 10, UNICEF's children's rights and business, available at: <https://www.unicef.org/csr/47.htm> (last visited 08 May 2017).

²³⁴ UNICEF Guidelines for Industry on Child Online Protection (2015), available at: https://www.unicef.org/csr/css/COP_Guidelines_English.pdf (last visited 08 May 2017).

material.²³⁵ Such practices as blocking content, splash notifications and report mechanisms are named as an effective tools used by companies to fulfil this responsibility.²³⁶

Close partnership with IT companies as a whole and major search engines in particular has been named as one of the most important tools to combat the spread of child sexual abuse materials on the Internet during the ECPAT World Congress III against Sexual Exploitation of Children and Adolescents.²³⁷ Despite growing number of illegal activities being concentrating on the dark web, web-based searches of indexed content remain to be the one of the most frequently used tools to obtain child sexual abuse and exploitation materials. Image hosts are also important as they contain significantly more abuse material than other resources.²³⁸ Moreover, as IWF's report shows, there had been 21% increase in URL's contained child sexual abuse content in 2016.²³⁹ Thus it seems relevant to analyse the contributions made by IT companies and potential for broader and more coordinated collaboration.

It can be claimed that IT companies are rather active in cooperating with global NGOs and government agencies for the purpose of protecting children. Examples of such would be contributions of Microsoft and Google as the research conducted by Steel shows that the blocking efforts undertaken by these companies lead to 67% drop in searches of child sexual exploitation materials over 2014.²⁴⁰ Yet, the same report shows that another large search engine, Yandex, did not implemented similar measures as neither possession nor viewing are not criminalised in Russia where the engine is based.²⁴¹ Therefore there had been no changes in search rates for child sexual abuse and exploitation materials on Yandex that was used not only by Russian paedophiles, but also those from United States²⁴² with the approximately 60 million queries per month.²⁴³

²³⁵ UNICEF Guidelines for Industry on Child Online Protection (2015).

²³⁶ UNICEF Guidelines for Industry on Child Online Protection (2015).

²³⁷ ECPAT International Report on The World Congress III against Sexual Exploitation of Children and Adolescents (2009), available at:

http://www.ecpat.org/wp-content/uploads/legacy/ECPATWCHIIReport_FINAL.pdf (last visited 10 May 2017).

²³⁸ IWF 2016 Annual Report, available at: https://annualreport.iwf.org.uk/assets/pdf/iwf_report_2016.pdf (last visited 22 May 2017).

²³⁹ IWF 2016 Annual Report.

²⁴⁰ C.M.S. Steel, "Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms", *Child Abuse & Neglect* (2015).

²⁴¹ *Ibid.*

²⁴² *Ibid.*

²⁴³ *Ibid.*

There are other practices, applied by IT companies to combat child sexual abuse or exploitation materials on the Internet. Thus, Google and Microsoft use sets of special hashes (“*unique signatures based on a mathematical function that can be generated for previously identified child pornographic images and movies*” as Steel puts it)²⁴⁴ to identify child pornography in webmail and Google Drive/OneDrive storage areas, followed by notification of law enforcement agencies.²⁴⁵ Contributions from users through report mechanisms are also of high value. Thus, for example, on Facebook every user has an opportunity to report child sexual abuse or exploitation materials. Splash pages that appear when the user conducts search for illicit material, are yet another example of collaboration between law enforcement agencies and IT companies, INTERPOL worst-of list being one of the most prominent illustration. Splash pages may contain the information on laws on child pornography, including penalties for possession and viewing it, links to relevant legislation or an encouragement to seek help as it was noticed by Nouwen.²⁴⁶ Such notification can have fear users from the page²⁴⁷, raise awareness²⁴⁸ or even reduce the normalisation of the offence²⁴⁹.

Yet it is important to keep in mind as it had been noted by ECPAT cooperation between law enforcement agencies and IT companies remains voluntarily,²⁵⁰ as international law does not impose obligations directly on companies. While Ruggie principles and UNICEF Guidelines, are being respected by the largest IT companies, CSR remains a moral responsibility. It is even recommended to specifically state that collaboration is not “anti-technology” or “anti-business” to get companies to participate in such partnerships,²⁵¹ though most of the IT companies take CSR and collaboration to combat child pornography rather seriously.²⁵² Still,

²⁴⁴ C.M.S. Steel, “Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms”, *Child Abuse & Neglect* (2015).

²⁴⁵ V. McKalin “Microsoft followed Google by tipping off police about child porn user on OneDrive”, (2014) cited by C.M.S. Steel, “Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms” (2015).

²⁴⁶ Y. Nouwen “The Effectiveness of Splash Pages as a Deterrence Measure”, *ECPAT Journal*, Issue 12 (2017), available at: http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf (last visited 12 May 2017).

²⁴⁷ *Ibid.*

²⁴⁸ *Ibid.*

²⁴⁹ E. Quayle, M. Taylor “Child pornography and the Internet, perpetuating a cycle of abuse”, *Deviant Behavior*, 23 (4) (2015) cited by Y. Nouwen “The Effectiveness of Splash Pages as a Deterrence Measure” (2017).

²⁵⁰ ECPAT International Report on The World Congress III against Sexual Exploitation of Children and Adolescents (2009).

²⁵¹ *Ibid.*

²⁵² See, for example, N. Pickles, Head of UK Public Policy on Twitter cited in IWF 2016 Annual Report, available at: https://annualreport.iwf.org.uk/assets/pdf/iwf_report_2016.pdf (last visited 22 May 2017.)

in absence of clear and effective regulations, obligations taken by companies may vary as it is seen from Steel research on Google, Bing and Yandex. Such differences lead to emergence of loopholes that are being actively used by offenders. Therefore, there is a pressing need for regulations on this sector in order to harmonise approaches taken by companies. Nevertheless, one should keep in mind that it would only be a part of a solution as there is an increasing trend of moving child sexual abuse materials to the darknet, that remains unregulated. Here, however, the notion of the pressure from the civil society can play its role as the dark web not only consists of web resources for illicit activities. As it was previously noted, software used to reach the darknet is mostly legal and widely available. Thus, companies operating such technologies can be encouraged to take part in various agreements aimed at the combating child sexual abuse materials. It has been noticed by researchers that individuals operating on the dark web tend to actively oppose and take down child sexual abuse.²⁵³ The example of such would be users of the Dark Web Social Network analysed by Gehl.²⁵⁴ Coming back to Quayle and Taylor's suggestion that awareness raising and education among general population could lead to decrease in normalisation of viewing child sexual abuse or exploitation materials,²⁵⁵ the work of NGOs appears to be a rather powerful solution tool that is addressed in a next subchapter.

Alongside our peers, Twitter is committed to eradicating child sexual exploitation content online. Our membership of the Internet Watch Foundation is an extremely important part of this mission, allowing us to work with industry peers and the IWF's experts to ensure we are innovating and adapting to the behaviour of perpetrators. We're proud to stand alongside the IWF, and continue to support them in their critical mission to safeguard children."

²⁵³ R. W. Gehl "Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network" (2016).

²⁵⁴ *Ibid.*

²⁵⁵ E. Quayle, M. Taylor "Child pornography and the Internet, perpetuating a cycle of abuse", *Deviant Behavior*, 23 (4) (2015) cited by Y. Nouwen "The Effectiveness of Splash Pages as a Deterrence Measure" (2017).

4.6 Awareness and Advocacy: Role of Civil Society and NGOs

While there is a clear need for a new, more strict regulations on the matter, it should not gone unnoticed that states do have obligation of a jus cogens nature to protect children from all for forms of abuse, including sexual abuse regardless of it's being committed online or offline. To reach the point of effective protection, steps must be taking national legislations must be harmonised, thus strictly prohibiting viewing the materials. These steps are secured under the international and regional instruments that present to be a rather good tool in combating the crime of viewing child sexual abuse materials. Not only states are required to take a unified approach to the issue, but also business, specifically IT sector, as well as society as a whole. There is a pressing need to take action and do it as soon as possible. To convince states, business sector and general public to get more serious attitude towards the problem, strong advocacy is needed. Civil society and international NGOs plays a major role in that process, thus it seems necessary to address the solutions from that perspective as well.

The importance of NGO involvement in a process of combating child sexual abuse or exploitation materials on the Internet had been highlighted by researchers for over the decade. Thus, Carr calls for more active collaboration between academia, NGOs, tech industry and law enforcement sector, naming a new, truly global NGO as a part of the solutions in combating child pornography.²⁵⁶ Carr points out the value of public accountability claiming that it is a crucial feature in international work in order to secure a high level of political priority.²⁵⁷ Here one can see an important notion of the work of civil society, namely, support of a political interest in the area. Such collaborations have been made, thus, for example, UNICEF among others, is working with governments, civil society and business in order to promote children's rights related to the Internet and associated technologies.²⁵⁸ Indeed, child

²⁵⁶ J. Carr "Out of sight, out of mind' Tackling child sex abuse images on the internet – a global challenge" (2006).

²⁵⁷ *Ibid.*

²⁵⁸ UNICEF "Children's rights and the Internet", available at: <https://www.unicef.org/csr/childrensrighsandinternet.htm> (last visited 08 May 2017).

sexual abuse is taken more and more seriously by governments these days, however, it is still unbalanced as many countries have other priorities on their agenda.

Creation of a public monitoring mechanisms and hotlines done by some NGOs²⁵⁹ working on the issue, appears to be a powerful tool to engage public into the process of combating child sexual abuse and exploitation materials on the Internet. Thus, 105,420 reports were processed by IWF analysts in 2016 resulting in removing of 57,335 web pages containing child sexual abuse images or videos.²⁶⁰ The numbers, however, are in decrease in relation to those of 2015, probably because of the growing tendency for the offenders to use darknet resources which are much more difficult to remove. Though IWF report shows a decrease in numbers of a new darknet resources,²⁶¹ that does not mean that those discovered previously had not been used by offenders. Thus, despite report mechanisms being a successful tool in combating the offence, there is still need to broader education and awareness rising to reach broader public, including those regularly operating the dark web. It is of importance, however, not to overgeneralise darknet users as they are reaching the dark web for various purposes, not only for illicit activities.

Awareness raising and the availability of statistics made by most of NGOs are of help in relation to this problem. Thus, for example, IWF 2016 Report claims that a decrease of newly identified hidden services could be due to increased awareness by law enforcement internationally about hidden services distributing child sexual abuse imagery.²⁶² Another example of awareness raising practices would be the Safer Internet Centres organised by pan-European network called INSAFE setting up awareness centres and helplines in different countries. Together, networks are organising Safer Internet Day, that is aimed to reach a wide public, and is a quite successful initiative.²⁶³ In Denmark, Save the Children ran a campaign targeting human resource managers in 98 local municipalities encouraging reporting to the Danish national hotline of child pornography discovered on workplace servers.

²⁵⁹ For example, IWF, ECPAT, NCMEC, INHOPE are collaborating with law enforcement agencies and provide public with an opportunity to anonymously report child sexual abuse materials on the Internet.

²⁶⁰ IWF 2016 Annual Report, available at: https://annualreport.iwf.org.uk/assets/pdf/iwf_report_2016.pdf (last visited 22 May 2017).

²⁶¹ *Ibid.*

²⁶² *Ibid.*

²⁶³ Thus, in 2016, Safer Internet Day messages reached a 2 in 5 young people (8-17s) and 1 in 5 parents in the UK. See IWF 2016 Annual Report, available at: https://annualreport.iwf.org.uk/assets/pdf/iwf_report_2016.pdf (last visited 22 May 2017).

It can be seen that there is a growing trend of cooperation between states, NGOs and ISPs on the matter of reporting and taking down web resources containing child sexual abuse materials. International Association of Internet Hotlines (INHOPE)²⁶⁴ being one of the most prominent examples of this. INHOPE is a network of 51 hotlines in 45 countries worldwide that is committed to stamping out child pornography from the Internet. Thus, in Germany due to collaboration with INHOPE only in 2013 99% of more than 4000 websites hosted in Germany containing child pornography were deleted within one week.²⁶⁵ Still, more of such collaborations are needed not only to target websites located on the surface web, but also on the darknet. Thus, there is a need for a significant amount of investments, pointed out already by Carr in 2006,²⁶⁶ and presenting to be relevant to the moment due to the ever-developing technologies used by offenders.²⁶⁷

Media can also play a significant role in the awareness rising, the example of which can be seen in research conducted by Aftonbladet and Svenska Dagbladet in 2016.²⁶⁸ Following this study, the debates on the gravity of the issue had been reinitiated in a Swedish society.²⁶⁹ That in turn led to increased cooperation between the government and ECPAT Sverige as the Minister of Justice recently visited ECPAT facilities and made a statement on the seriousness of the problem.²⁷⁰ The actual outcomes, however, remain unknown as the development is very recent. Still, it is possible to claim that the level of awareness on child sexual abuse materials on the Internet indeed has been raised.

Summarising, it is evident that civil society makes a significant contribution to combat child sexual abuse materials on the Internet. Awareness raising and statistics that are made available for the public motivate governments take a more serious approach towards the issue

²⁶⁴ Available at: <http://www.inhope.org/gns/who-we-are/at-a-glance.aspx> (last visited 17 May 2017).

²⁶⁵ Global Alliance Against Child Sexual Abuse Online 2015 Report, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_2015_report_en.pdf (last visited 17 May 2017).

²⁶⁶ J. Carr "Out of sight, out of mind" Tackling child sex abuse images on the internet – a global challenge" (2006).

²⁶⁷ Global Alliance Against Child Sexual Abuse Online 2015 Report.

²⁶⁸ Aftonbladet "15 000 laddade ned – bara 119 dömdes" (2017).

²⁶⁹ Parliamentarians' opinions are available (in Swedish) at: <http://www.aftonbladet.se/nyheter/a/bPnKv/riksdagsmajoritet-for-lagandring> (last visited 25 April 2017).

²⁷⁰ Available at (in Swedish): http://www.ecpat.se/blogg/2017/04/26/morgan-johansson-att-bevittna-oevergreppsmaterial-paverkar-maenniskor-pa-olika-saett-nu-naer-jag-sett-detta-kaenner-jag-ilska?utm_source=Facebook&utm_medium=Sponsrat+inl%C3%A4gg&utm_campaign=Morgan+Johansson+ECPAT+Hotline (last visited 12 May 2017).

and provoke public discussion on the matter. Educational means are also of importance as they are contributing to safer Internet for both children and adults. There had been increase in collaboration between law enforcement agencies, governments and NGOs during the recent years. That resulted in creation of report mechanisms that turned to be a powerful tool in blocking web resources containing child pornography. Still, in the light of constantly evolving technologies that are actively used by offenders, more collaboration is needed. Reducing normalisation of viewing child sexual abuse or exploitation materials on the Internet appears to be one of the essential elements of public education, as there is still a trend to consider viewing an unharmed and victimless activity.

Concluding Remarks

Zero tolerance is crucial when it comes to any abuse of children²⁷¹.

It has been noted by the Council of Europe Commissioner for Human Rights that “*sexual assault against children is an urgent human rights issue and fighting it should be a political priority*”.²⁷² Yet, despite all the apparent developments on the field, the notion of viewing child sexual abuse still widely falls out of the scope of legislators. That, as I argued during this thesis, cannot continue as it leads to multiplication of the abuses, increased demand for the production, dehumanises and gravely damages real children. The number of offenders, using various technological tools to access child sexual abuse and exploitation materials is growing rapidly alongside with figures of crimes of international character, since the Internet allows perpetrators to connect with foreign peers and obtain an access to material located in another country. It also contribute to normalising the offence, often resulting in a further abuse of children, thus being a threat to children’s rights and public morals. Accordingly, the the violence of the abuses increases alongside with the demand for new material. These crimes certainly affect children that had been abused, as well as those who are exposed to such kind of material in a process of grooming. Despite all the efforts to track down web resources containing child sexual abuse materials, materials are multiplied so many times, that they tend to stay on the Internet as long as it is going to exist, even though websites are being taken down by aw enforcement agencies with the help of ISPs and civil society. Children, once abused and exploited for the production of the materials are being re-victimised every time the material is viewed. Their dignity, privacy and health being gravely affected by the abuse itself and the constant reappearance of the materials. That, in turn, leads to severe consequences of person’s development, perpetual feeling of fear and anxiety sometimes resulting in suicides. The harm caused to children by such dehumanising acts is real, thus,

²⁷¹ T. Hammarberg “Zero tolerance for sexual abuse of children” (2011), available at: <http://www.coe.int/hr/web/commissioner/-/zero-tolerance-for-sexual-abuse-of-childr-1> (last visited 09 May 2017).

²⁷² *Ibid.*

there is a need of criminalisation of the offence of viewing child sexual abuse materials on the Internet.

With the evolving of encryption and anonymising tools, law enforcement agencies seem to find themselves one step behind the offenders, even though there've been some achievements on the field due to collaboration between them, as well as with IT sector. Yet efforts put by states into the problem are not sufficient in a situation of rapid globalisation of the offence. Due to the global nature of the phenomenon of viewing child sexual abuse materials, the number of situations of several states claiming jurisdiction over the crime are going to increase. That is further aggravated by rather diverse approaches towards the offence of child sexual abuse or exploitation as a whole and the notion of viewing in particular taken by the states even though they had ratified same international legal instruments. In absence of clear regulations, it results in prolongation of disputes between the states and often impossibility to prosecute the offence. Same comes up with the issue of unknown location of the materials, which is often the consequence of usage of ICT by perpetrators. Inadequacy of national and regional legislation, and case-law, inconsistency in language of major instruments on the issue as well as the option to make a reservation on such an important provisions as definitions of a child, types of materials and crimes, only add to the complexity of the problem. Differences in legislation between the states also lead to large delays in investigation process, lose of evidences in parts or fully. All of that allows the vast majority of the incidents go unprosecuted as it was illustrated by the Swedish study,²⁷³ with other researches show that there is a trend that the number of offences of viewing child sexual abuse or exploitation materials on the Internet will only continue to grow.²⁷⁴

Thus, there is a need for international community to take more complex approach towards the crimes of viewing child sexual abuse materials on the Internet, starting with the elimination of loopholes in national legislations. With the ease that one can view the materials due to evolving technologies, the offence of viewing child sexual abuse or exploitation materials on the Internet must be taken as seriously as any other offence of child pornography, thus it should be criminalised and prosecuted. Providing clear definitions either with the use of commentary to the existing instruments, or with the new treaty, is also of urgent importance.

²⁷³ The study made by Aftonbladet and Svenska Dagbladet "15 000 laddade ned – bara 119 dömdes" (2017).

²⁷⁴ Global Alliance Against Child Sexual Abuse Online "2015 Threat Assessment Report" (2015).

Global effort in crime prevention is also needed in response for the global problem. The collaboration on the matter must, therefore, be more active and sincere, since the cooperation between offenders due to peer-to-peer networks and use of various technological means remains more advanced allowing them to escape prosecution. Education and further training in ICT for law enforcement officers should be available to enable them to investigate such type of crimes, thus a particular amount of investment is needed.

That said, the notion of the balance of rights should be taken into account. Thus, the means and methods used in the investigation and crime-prevention processes must be evaluated to not to be the surveillance technology. Still, one should keep in mind that scope of the offence of viewing child sexual abuse or exploitation materials on the Internet and gravity of the consequences for victims. Contributions made by ISPs and the IT sector should be used when possible, however, there is a need for more harmonised guidelines and regulatory mechanisms as for now all the cooperation is done on a voluntary, virtually unregulated basis.

The problem also calls for rising awareness among general public, civil society and governments, and it's a task of international community to make states to fulfil their obligations to protect children's rights secured under the international law.

Bibliography

Books

Akdeniz, Y. (2008). *Internet Child Pornography and the Law: National and International Responses*. Ashgate.

Buck, T. (2011). *International Child Law*. 2nd ed. London: Routledge.

Foucault, M. (1991) [1979] Panopticism. In: *Discipline and Punish: The Birth of the Prison*. London: Penguin, pp. 195-219.

Freeman, M. (1997). *The Moral Status of Children: Essays on the Rights of the Children*. Martinus Nijhoff Publishers.

Gillespie, A. (2011). *Child Pornography: Law and Policy*. Abingdon: GlassHouse/Routledge.

Kant, I. (1780). *The metaphysical elements of ethics*.

Martellozzo, E. (2012). *Online Child Sexual Abuse. Grooming, Policing and Child Protection in a Multi-Media World*. Abingdon: Routledge.

Nozick, R. (1974). *Anarchy, State and Utopia*. New York: Basic Books.

Palmer, T. and Stacey, L. (2004). *Just One Click: Sexual Abuse of Children and Young People Through the Internet and Mobile Telephone Technology*. London: Barnado's.

Svedin, C.G. and Back, K. (1996). *Children who don't speak out. About children being used in child pornography*. Rädda Barnen Sweden.

Turkle, S. (1995). *Life on the screen: identity in the age of the Internet*. New York: Simon and Schuster.

van Bueren, G. (1998). *The International Law on the Rights of the Child*. Martinus Nijhoff Publishers.

von Hirsch, A. (1993). *Censure and Sanctions*. Oxford: Clarendon.

Articles and publications

Abel, G.G. (1985). *Use of pornography and erotica by sex offenders*. Paper presented to the United States Attorney General's Commission on Pornography, Houston, TX.

Abelson, H. et al. (2015). Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 2015:1-11.

Aftonbladet (2017). *15 000 laddade ned – bara 119 dömdes*, available at: <http://anvandarna.story.aftonbladet.se/chapter/15-000-laddade-ned-bara-119-domdes/> (last visited 15 May 2017).

Aftonbladet (2017). *Riksdagsmajoritet för lagändring*, available at: <http://www.aftonbladet.se/nyheter/a/bPnKv/riksdagsmajoritet-for-lagandring> (last visited 25 April 2017).

Akdeniz, Y. and Strossen, N. (2000). Sexually oriented expression. In Y. Akdeniz, C. Walker, D. Wall (eds.): *The Internet, Law and Society*. Harlow: Longman, pp. 207-231.

Albury, K. and Crawford, K. (2012). Sexting, Consent and Young People's Ethics: Beyond Megan's Story. *Continuum: Journal of Media and Cultural Studies*, 26(3): 463-473.

Ball, J. (2014). Guardian launches SecureDrop system for whistleblowers to share files. *Guardian*, available at: <https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistle-blowers-documents> (last visited April 2017)/

BBC News (2001). Wickedness of Wonderland, available at: http://news.bbc.co.uk/2/hi/uk_news/1167879.stm (last visited 28 April 2017).

Bedau, H.A. (1984). Classification-Based Sentencing: Some Conceptual and Ethical Problems. *New England Journal of Criminal and Civil Confinement* 10(1): 1-26.

Bradbury, D. (2004). Unveiling the dark web. *Network Security*, 2014(4): 14–17.

BrightPlanet (2014). *Clearing Up Confusion - Deep Web Vs. Dark Web*, available at: <http://www.brightplanet.com/2014/03/clearing-confusion-deep-web-vs-darkweb/> (last visited 26 April 2017).

Calvert, C. (2009). Sex, Cell Phones, Privacy, and the First Amendment: When Children Become Child Pornographers and the Lolita Effect Undermines the Law. *CommLaw Conspectus*, 18(1): 1-65.

Carr, J. (2006). 'Out of sight, out of mind': Tackling child sex abuse images on the internet – a global challenge. *UK: Children's Charities' Coalition on Internet Safety*, available at: <http://www.chis.org.uk/2006/07/24/-out-of-sight-outof-mind-tackling-child-sex-abuse-images-on-the-internet-a-global-challenge-> (last visited 22 May 2017).

Carr, J. and Hilton, Z. (2011). Combating child abuse images on the Internet: International perspectives. In J. Davidson and P. Gottschalk (eds.): *Internet Child Abuse. Current Research and Policy*. New York: Routledge, pp. 52-78.

ECPAT International (2009). *Report on The World Congress III against Sexual Exploitation of Children and Adolescents*, available at:

http://www.ecpat.org/wp-content/uploads/legacy/ECPATWCIIIReport_FINAL.pdf (last visited 10 May 2017).

ECPAT International (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, available at: <http://www.ecpat.org/resources> (last visited 12 May 2017).

ECPAT International “Online Child Sexual Abuse and Exploitation. An Analysis of Emerging and Selected Issues” (2017), available at:

http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf (last visited 20 May 2017).

ECPAT Sverige (2017). *Barnpornografibrottet. Det straffrättsliga skyddet mot dokumenterade sexuella övergrepp mot barn*, available at:

http://www.ecpat.se/uploads/ECPAT_Barnpornografibrottet_2017.pdf (last visited 08 May 2017).

ECPAT Sverige (2011). *The Commercial Sexual Exploitation of Children*, available at: <http://www.mynewsdesk.com/se/ecpat/documents/ecpat-the-commercial-sexual-exploitation-of-children-13882> (last visited 13 May 2017).

ECPAT Sverige(2017). “*Morgan Johansson: ”Att Bevittna Övergreppsmaterial Påverkar Människor på Olika Sätt. Nu När Jag Sett Detta Känner Jag Ilska”*”

Available at:

http://www.ecpat.se/blogg/2017/04/26/morgan-johansson-att-bevittna-oevergreppsmaterial-paverkar-maenniskor-pa-olika-saett-nu-naer-jag-sett-detta-kaenner-jag-ilska?utm_source=Facebook&utm_medium=Sponsrat+inl%C3%A4gg&utm_campaign=Morgan+Johansson+ECPAT+Hotline (last visited 12 May 2017).

Eneman, M. (2005). *The New Face of Child Pornography*. In M. Klang and A. Murray (eds.): *Human Rights in the Digital Age*. London: GlassHouse Press, pp. 27-40.

Eneman, M. (2012). *Access Blocking of Child Abusive Material: Evaluation of the Swedish Practice*. Conference Proceedings of the 4th International Symposium on Children at Risk and in Need of Protection, available at: <https://gup.ub.gu.se/publication/156041> (last visited 12 May 2017).

Eneman, M. (2016). *Internet Filtering – A legitimate control mechanism of criminal behaviour in the digital society? Stockholm Criminology Symposium*.

Falconer, J. (2012). *Mail-Order Drugs, Hitmen & Child Porn: A Journey into the Dark Corners of the Deep Web*. *Next Web* (Oct. 8, 2012, 2:56 AM), available at: <http://thenextweb.com/insider/2012/10/08/mail-order-drugs-hitmen-child-porn-a-journey-into-the-dark-corners-of-the-deep-web/> (last visited 27 April 2017).

- Farivar, C. (2016). Once more, a judge rules against gov't in Tor-enabled child porn case. *Arstechnica*, available at: <https://arstechnica.com/tech-policy/2016/05/once-more-a-judge-rules-against-govt-in-tor-enabled-child-porn-case/> (last visited 12 May 2017).
- Fathaigh, R. (2011). Child Pornography and Freedom of Expression. *Strasbourg Observers*, available at: <https://strasbourgobservers.com/2011/10/10/child-pornography-and-freedom-of-expression/> (last visited 10 May 2017).
- Gehl, R.W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New media & society*, 18(7):1219–1235.
- Gillan, A. (2003). Race to Save New Victims of Child Pornography. *Guardian*, 4 November 2003.
- Gillespie, A. (2003). The Sexual Offences Act 2003: Tinkering with Child Pornography. *Criminal Law Review*, 3:361-368.
- Gillespie, A. (2013). Adolescents, sexting and human rights. *Human Rights Law Review*, 13 (4): 623-643.
- Global Alliance Against Child Sexual Abuse Online (2015). *2015 Threat Assessment Report*, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_threat_assessment_en.pdf (last visited 22 May 2017).
- Gutheil, M. et al. (2017). *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, available at: <http://www.europarl.europa.eu/supporting-analyses> (last visited 28 April 2017).
- Haasz, A. (2016). Underneath It All: Policing International Child Pornography on the Dark Web. *Syracuse Journal of International Law & Commerce*. 43(2):353-380.
- Hammarberg, T. (2011). Zero tolerance for sexual abuse of children. *Human Rights Comment: Commissioner for Human Rights, Council of Europe*, available at: <http://www.coe.int/hr/web/commissioner/-/zero-tolerance-for-sexual-abuse-of-childr-1> (last visited 09 May 2017).
- Hampton, J. (1995). How You Can Be Both a Liberal and a Retributivist: Comments on Legal 'Moralism and Liberalism' by Jeffrie Murphy. *Arizona Law Review*, 37: 105–116.
- Harvard Law Review (2009). Child Pornography, The Internet, and the Challenge of Updating Statutory Terms, 2009/06/01, Vol: 122, pp. 2206-2227.

Hildebrandt, M. (2016). Law as Information in the Era of Data-Driven Agency. *The Modern Law Review*, 79(1): 1-30.

Hughes, D. M. (2000). The internet and sex industries: partners in global sexual exploitation. *Technology and Society Magazine*, 19(1): 35-42.

Human Rights Watch (2006). *Race to the Bottom. Corporate Complicity in Chinese Internet Censorship*, available at: https://www.hrw.org/reports/2006/china0806/3.htm#_Toc142395820 (last visited 26 April 2017).

IACP Summit Report (2015). *Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence*, available at: www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf (last visited 20 May 2017).

ICMEC (2016). *Child Pornography: Model Legislation & Global Review*, available at: <http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf> (last visited 20 May 2017).

INTERPOL (2017) *Global operation targets child sexual abuse material exchanged via messaging apps*, available at: <https://www.interpol.int/News-and-media/News/2017/N2017-047> (last visited 12 May 2017).

IWF (2014). *Annual Report 2014*, available at: <https://www.iwf.org.uk/sites/default/files/reports/2016-02/IWF%202014%20Annual%20Report%20%28web%29.pdf> (last visited 20 May 2017).

IWF (2016). *Annual Report 2016*, available at: https://annualreport.iwf.org.uk/assets/pdf/iwf_report_2016.pdf (last visited 22 May 2017)

Matravers, M. (2011). Is Twenty-First Century Punishment Post-Desert? In M. Tonry (ed.): *Retributivism Has a Past: Has It a Future?* Oxford University Press, pp. 30–45.

McKalin, V. (2014). Microsoft followed Google by tipping off police about child porn user on OneDrive. *Tech Times*, available at: <http://www.techtimes.com/articles/12475/20140809/microsoft-followed-google-by-tipping-of-f-police-about-child-porn-user-on-onedrive.htm> (last visited 20 May 2017).

Meduza (2016). Роскомнадзор заблокировал мой любимый сайт, что делать? [Roskomnadzor has blocked my favorite website, what should I do?], available at: <https://meduza.io/feature/2016/09/15/roskomnadzor-zablokiroval-moy-lyubimyy-sayt-chno-delat> (last visited 10 May 2017).

Neal, M. (2013). To Bust a Giant Porn Ring, Did the FBI Crack the Dark Web?. *Vice*, available at:

<http://motherboard.vice.com/blog/the-fbi-says-it-busted-the-biggest-child-porn-ring-on-the-deep-web-1> (last visited 27 April 2017).

Nouwen, Y. (2017). The Effectiveness of Splash Pages as a Deterrence Measure. *ECPAT Journal*, 12, available at: http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf (last visited 12 May 2017).

O'Neill, P.H. (2013). An In-Depth Guide to Freedom Hosting, the Engine of the Dark Net. *Daily Dot* (Aug. 4, 2013), available at: <https://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/> (last visited 20 May 2017).

Owen, G. and Savage, N. (2015). The Tor Dark Net. *Centre for International Governance Innovation and the Royal Institute of International Affairs*, available at: https://www.ourinternet.org/sites/default/files/publications/no20_0.pdf (last visited 05 May 2017).

Quayle, E. and Taylor, M. (2003). Model of Problematic Internet Use in People with a Sexual Interest in Children. *Cyber Psychology and Behavior*, 6(1): 93-106.

Quayle, E. and Taylor, M. (2003). *Child Pornography: An Internet Crime*. Routledge.

Quayle, E. and Taylor, M. (2015). Child pornography and the Internet, perpetuating a cycle of abuse. *Deviant Behavior*, 23(4): 331-361.

Quayle, E., Taylor, M., and Holland, G. (2001). Child Pornography, the Internet and Offending. *The Canadian Journal of Policy Research*, 2: 94-100.

Quayle, E., Loof, L., and Palmer T. (2008). Child Pornography and Sexual Exploitation of Children Online. A contribution of ECPAT International to the World Congress III against Sexual Exploitation of Children and Adolescents Rio de Janeiro, Brazil 25-28 November 2008, available at:

http://resources.ecpat.net/worldcongressIII/PDF/Thematic/CHILD_ABUSE_IMAGES_concept_note.pdf (last visited 20 May 2017).

Ripstein, A. (2006). Beyond the Harm Principle. *Philosophy & Public Affairs*, 34(3): 215-245.

Silbert, M.H. (1989). The Effects on Juveniles of Being Used for Pornography and Prostitution. Child Pornography and Sex Rights. In D. Zillmann and J. Bryant (eds.): *Pornography: Research Advances and Police Considerations*. Hillside, NJ: Lawrence Erlbaum Press, pp. 215-234.

Silbert, M.H. and Pines, A.M. (1984). Pornography and Sexual Abuse of Women. *Sex Roles*, 10(11/12): 857-868.

- Steel, C.M.S. (2015). Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child Abuse & Neglect*: 1-9.
- Tomlin, P. (2014). Retributivists! The Harm Principle Is Not for You! *Ethics*, 124(2): 272-298.
- Walker, S. (2015). Russian data law fuels web surveillance fears. *Guardian*, available at: <https://www.theguardian.com/world/2015/sep/01/russia-internet-privacy-laws-control-web> (last visited 28 April 2017).
- Weisberg, D.K. (1984). The “Discovery” of Sexual Abuse: Experts’ Role in Legal Policy Formation. *Univ. of California Davis Law Review*, 18: 1-57.
- Weinstein, J. (2011). “Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes”, Statement before the Committee on Judiciary Subcommittee on Crime, Terrorism, and Homeland Security United States House of Representatives.
- Wolak, J, Mitchell, K., and Finkelhor, D. (2003). Internet Sex Crimes Against Minors: The Response of Law Enforcement. In K. Kendall-Tackett and S. Giacomoni (eds.): *Child victimization*. Kingston, NJ: Civic Research Institute, pp. 2.1-2.17.

Legal and semi-legal documents

- American Convention on Human Rights (1969)
- African Charter on the Rights and Welfare of the Child (1990)
- Charter of Fundamental Rights of the European Union
- Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) (1950)
- Council of Europe Convention on Cybercrime (2001)
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007)
- Directive 2011/92/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, European Union (2011)
- EUROPOL and ENISA (2016). *Joint Statement on lawful criminal investigation that respects the 21st Century data protection*.
- Explanatory Report, Convention on Cybercrime (2001)

HIPSSA – Cybercrime directive: Explanatory notice – Economic Community of West African States (2013)

ILO Convention Concerning Minimum Age for Admission to Employment, No 138, (1973)

ILO Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour, No. 182 (1999)

International Covenant on Civil and Political Rights (1966)

International Covenant on Economic, Social and Cultural Rights (1966)

INTERPOL (2011). *GA Resolution “Combating online sexual exploitation of children through a legislative global engagement strategy”*, AG-2011-RES-05

INTERPOL (2009). *GA Resolution “Combating sexual exploitation of children on the Internet using all available technical solutions, including access-blocking by INTERPOL member countries”*, AG-2009-RES-05

INTERPOL. *Crimes Against Children, Access blocking*. Available at:

<https://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking> (last visited 12 May 2017)

Kaye, D. (2016), Report submitted by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38

Maala, N.M. (2009). Report submitted by the Special Rapporteur on the sale of children, child prostitution and child pornography, A/HRC/12/23

Petit, J.M. (2004). Rights of the Child: Report submitted by the UN Special Rapporteur on sale of children, child prostitution and child pornography. *UN Economic and Social Council*, 2004, E/CN.4/2005/78

Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography (2000)

Universal Declaration of Human Rights (1948)

UNICEF. *Children's rights and business*, available at: <https://www.unicef.org/csr/47.htm> (last visited 08 May 2017)

UNICEF. *Children's rights and the Internet*, available at:

<https://www.unicef.org/csr/childrensrightsandinternet.htm> (last visited 08 May 2017)

UNICEF (2015). *Guidelines for Industry on Child Online Protection*, available at:

https://www.unicef.org/csr/css/COP_Guidelines_English.pdf (last visited 08 May 2017)

UN (2002). *A World Fit for Children*. (UN Doc. GA/RES/S-27/2, 2002)

UN Convention on the Rights of the Child (1989)

UN General Assembly (2016). *The right to privacy in the digital age*, A/C.3/71/L.39/Rev.1

UN HR council (2011) *Guiding principles on business and Human Rights: Implementing the UN' "Protect, Respect and Remedy" Framework*, A/HRCH/17/31 (21 March 2011) (SRSG, Guiding Principles)

UN Office on Drugs and crime (2013). *Comprehensive Study on Cybercrime*, available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (last visited 20 May 2017)

Online resources

CEOP, available at: <https://www.ceop.police.uk/safety-centre> (last visited 17 May 2017)

Internet Watch Foundation, available at: <https://www.iwf.org.uk/> (last visited 20 May 2017)

INTERPOL on Crimes against children, available at: <https://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children> (last visited 20 May 2017)

Tor project, available at: <https://www.torproject.org> (last visited 26 April 2017)

Virtual Global Task Force, available at: <http://virtualglobaltaskforce.com> (last visited 17 May 2017)

Table of Cases

Court of Justice of the European Union (CJEU)

Judgment of the CJEU (Grand Chamber), *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 2014, joined cases C-293/12 and C-594/12

Judgment of the CJEU (Grand Chamber), *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 2016, joined cases C-203/15 and C-698/15

European Court of Human Rights (ECtHR)

ECtHR, *Cengiz and Others v. Turkey*, 2015, applications nos. 48226/10 and 14027/11

ECtHR, *Copland v. the United Kingdom*, 2007, application no. 62617/00

ECtHR, *Handyside v. the United Kingdom*, 1976, application no. 5493/72

ECtHR, *Karttunen v. Finland*, 2011, application no. 2872/02

ECtHR, *M.C. v. Bulgaria*, 2003, application no. 39272/98

ECtHR, *M.S. v. Sweden*, 1997, application no. 20837/92

ECtHR, *O'Carroll v. the United Kingdom*, 2005, application no. 35557/03

ECtHR, *Söderman v. Sweden*, 2013, application no. 5786/08

ECtHR, *X and Y v. the Netherlands*, 1985, application no. 8978/80

The United Kingdom case-law

Regina v. Harrison, 2008

Regina v. Porter, 2006

Regina v. Sharpe, 2001

Regina v. Smith, Regina v. Jayson, 2003

The United States case-law

Miller v. California, 1973

P.I. Ferber v. New York, 1982

United States v. Ackerman, 2016

United States v. Michaud, 2016

United States v. Osborne, 1991

United States vs R. W. Ulbricht (2013)