ICTs and Sexual Exploitation of Children in Europe

László Dornfeld
Ferenc Mádl Institute of Comparative Law, Hungary

INTRODUCTION

‘Child pornography’ is a negative social phenomenon directed against children who are a more vulnerable group of society due to their age, as they are still undergoing intellectual and moral development. It is also a global phenomenon just like cybercrime where the created material can be distributed anywhere in the world.

- With the advance of information technology, new methods of creating, acquiring and distributing child sexual exploitation material have begun to surface. The newest manifestation of this trend is the emergence of the so-called ‘virtual pornography’.
- The technology is relatively cheap, easy to access and portable. It allows for storage of large amounts of material, which would be conspicuous if stored in hard copy.
- Cyberspace provides an inexpensive and anonymous arena for offering, procuring, distributing, transmitting and sharing indecent pictures and videos, and represents an easy and very cheap way to access or obtain child pornography.
- As a result of advances in digital technology and the proliferation of information and communication technologies (ICTs), new forms of crime have emerged, many of which, like “outing and trickery sharing”, “repeated cyberstalking” or “snuff videos”, may overlap with child pornography offenses (Váradi-Csema, 2013, pp. 14-16).

The aim of this chapter is to outline the characteristics of child pornography, including the proper definition of the phenomenon. Then the next chapter discusses how ICTs transformed the production and distribution of child pornographic materials and how modern technology can help in covering the tracks of perpetrators. The chapter also addresses the new phenomenon of ‘virtual child pornography’. The last chapter is about the EU’s response to these criminal behaviors and new developments. The chapter mainly focuses on addressing European answers and regional level supranational legislation. National regulations may appear as examples in the text but not in-depth, taking the limited space of this chapter into consideration.

BACKGROUND

With each technological advance, the availability of child pornography was increasing, the latest being the Internet and ICTs (Quayle, 2011, p. 343). The origins of the development of child pornography can be traced back to the 1960s (Astinova, 2013, p. 4). Throughout these years, there was a gradual relaxation of laws regarding pornography (Gillespie, 2016, p. 227). For example, for almost a decade, all porno-

DOI: 10.4018/978-1-5225-9715-5.ch038

graphic materials were decriminalized in some North European countries, as there was only concern for the consumer and not for the circumstances of the production of these materials. Anti-pornography laws were repelled in 1969 in Denmark and in 1971 in Sweden (Quayle, 2011, p.343). The availability and distribution of child pornography through the Internet has become a social concern for society since the mid-1990s (Akdeniz, 2008, p. 1) The number of prosecutions in the UK involving indecent photographs of children increased from 93 in 1994 to 1,890 in 2003 (Clough, 2010, p. 248).

Sometimes it is questioned whether it is necessary to criminalize child pornography. Astinova argues that it has a preventive function because the demand for such materials provokes further child abuse and exploitation (Astinova, 2013, 4). In Gillespie's opinion, the harm caused to children is the primary reason, while later victimization due to the spread of such material is the secondary reason (Gillespie, 2016, p. 228). The question arises from these opinions: what about those materials which were produced without any victims (digital images, drawings or willing contributors)? This will be addressed later in the chapter.

Child pornography has changed drastically, industrial and technological advances have affected availability, photography, printing and distribution online (Taylor & Quayle, 2003; Aiken, Moran & Berry, 2011). As these materials can be accessed globally through the Internet, an international response is required, especially because of the jurisdictional challenges it raises (Gillespie, 2016, p. 231). In order to fight child pornography, different initiatives were adopted by the international and regional organizations such as the United Nations, the Council of Europe and the European Union (Herczeg, 2014, p. 70).

CHARACTERISTICS OF CHILD PORNOGRAPHY

The following chapters are focusing heavily on the regulations in various international and supranational instruments. Their territorial scopes differ significantly, as one is a global instrument while two were adopted by the Council of Europe (CoE) and thus include countries outside of the Europe Union and one is an EU Directive exclusively for Member States to observe. This means that the confusing situation caused by the already conflicting provisions is much worse.

- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (United Nations General Assembly Resolution A/RES/54/263 of 25 May 2000; 'OPSC')
- Convention on Cybercrime (Council of Europe, ETS No. 185 of 23 November 2001; 'Budapest Convention')
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Council of Europe, CETS No. 201 of 25 October 2007; 'Lanzarote Convention')
- EU Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography ('Directive 2011/93')

The UN's OPSC, an optional protocol to the Convention on the Rights of Child ('CRS'), although drafted in the digital age, pays little attention to the ICT-based abuse of children (Gillespie, 2016, p. 231). The CoE drafted the Budapest Convention as the first international treaty seeking to address Internet and computer crime by harmonizing national laws. As of the end of 2018, more than sixty countries joined the convention ('Council of Europe', 2018) which has a wide range of topics, focusing on both criminal law and criminal procedural law issues. It should not come as a surprise that child sexual exploitation only constitutes a small proportion of the content of the Convention and the only offense it covers is child pornography (Art. 9). As this was widely criticized, the Lanzarote Convention was adopted by the CoE to tackle all forms of child sexual exploitation (Gillespie, 2016, pp. 231-232).

The European Union had the Framework Decision 2004/68/JHA drafted as part of the 'third pillar' to combat child pornography on Union level but it was largely ineffective due to the limitations of EU's competence in criminal matters. After the Treaty of Lisbon came into effect in 2009, providing a clear mandate to deal with computer crime offenses, the EU has begun to rethink the existing legal regime on both policy and legal level (Buono, 2012, pp. 342-343). As a result of this process, the Directive 2011/93 was drafted, which is legally binding, meaning it is directly enforceable. Thus, it can be considered the "strongest" among the legal instruments.

Terminology

Sexual exploitation of children is a term for a wide range of sexual crimes involving children, like child prostitution or sex tourism. The most important aspect of the term in a digital environment is the creation and distribution of illegal material depicting sexual acts involving children. The proper terminology for describing this phenomenon is much disputed. 'Child pornography' is still widely used in legal documents while there is an emerging trend to replace it with other terms, including 'child sexual abuse material'. The reasoning behind this is that many find the word 'pornography' misleading, as it suggests mutual consent, some even going as far as stating that this wording "glorifies" the abusive content (Akdeniz, 2008, p. 11). The Virtual Global Taskforce states that labeling abusive material as 'pornography' legitimizes it and distances it from its criminal nature (Mathew, 2009). Some argue that the current terminology "creates a false distinction between the viewing of images and the contact sexual abuse of a child" ("PartnerSPEAK", 2015).

The European Parliament, in its Resolution on Child Sexual Abuse Online of 11 March 2015, stated that in the future 'child sexual abuse material' should be adopted as the correct terminology (2015/2564(RSP), Para. 12). The Terminology Guidelines drafted on 28 January 2016 by the Interagency Working Group on Sexual Exploitation of Children ('Luxembourg Guidelines') takes the middle ground and concludes that 'child pornography' is still used in legal documents but should be avoided outside of legal context (Greijer & Doek, 2016, p. 38).

This reasoning however is a bit too academic in nature as end material is tied so close to the act of abusing children that it is hard to believe society would become more accepting of the phenomenon just because of the terminology. Yes, some individuals or advocacy groups (like the infamous North American Man/Boy Lovers Association) might try to use it as a justification. There are also people who think positively of online piracy as they see it as a form of freedom from big corporations and there are even Pirate Parties in some national legislations but they rarely advocate for actual Somali pirates. A closer example would be the emergence of the term 'revenge porn', the disclosure of private sexual photographs or films, which also constitutes a criminal offense and so far, no one labeled it problematic or glorifying.

Moreover, the proposed replacement terms can also be misleading. For example, 'abuse' implicates that children must be harmed while making these materials, which is simply not true given recent developments, like virtual child pornography. In addition, it fails to take into consideration the increasing trend of children willingly producing these materials (Gillespie, 2012, pp. 3-4), as sexually active teenagers with a profound knowledge of ICTs are more likely to do so. This topic will be further explained in a later subtitle of the chapter. Although better solutions, as 'child exploitative material' can be coined (Gillespie, 2012, p. 4), the widely used 'child pornography' is still the most accurate term, so it will be used throughout the chapter.

Definition of Child Pornography

There are numerous different definitions of the notion in various international, supranational and national legal documents. The scope of differences varies from the use of proper terms to the materials included and methods of committing the crime. Three different factors must be taken into consideration when determining which materials can be considered child pornography. These are:

- Age of the person
- Type of the material
- Nature of the material

The first criterion refers to the person involved in the explicit material, more simply the age requirement to be considered a 'child'. The UN's CRS clearly states that all persons under the age of eighteen shall be protected (Art. 1), which provision also applies to its optional protocol, the OPSC. The CoE's Lanzarote Convention and Budapest Convention also extend protection to anyone under the age of eighteen but the latter also gives the opportunity for signatories to lower the age-limit to sixteen (Art. 9 para. 3). Lastly, the Directive 2011/93 defines 'child' as any person below the age of 18 years. On a policy-making level, this solution is the easiest to implement as people above this age are considered adults capable of consenting to be depicted in pornographic material. Deciding based on physical appearance (bodily developments associated with puberty) and psychological aspects could be a problematic task for law enforcement, as only a few victims are identified even today despite the great effort on the authorities' part, so deciding based on age can be considered the most appropriate method (Gillespie, 2016, pp. 233-235). Although there may be minors psychologically mature enough to give consent and fully understand the consequences of being filmed, ultimately only the person who creates the material will be in the position to know the circumstances of the production (Gilllespie, 2010, p. 205).

The biggest problem of age-based approach is the difference in age requirement between having consensual sexual intercourse and recording the act – even between spouses as the marriageable age is lower than 18 in some Member States. The age of consent differs from county to country: in Spain, it is 13 years, 14 years in Hungary (12 if both parties are minors), 15 years in the Czech Republic and 16 years in Belgium (Astinova, 2013, p. 11). The main reasoning behind this is the different consequences of having consensual sex and recording it, as the latter can be harmful to society and can boost the child pornography market (Clough, 2010, p. 257). In addition, it can be harmful for the individual too, as the recording can be posted on the Internet which later can yield search results when, for example, an employer is considering hiring the person. It can be argued that a sixteen-year-old is not ready to make such a decision and it was constantly done so by NGOs (Gillespie, 2012).

The second criterion concerns the type of material. Although we often associate pornography with visually depicting sexual acts, apparently there are other forms of it, like written texts and audio depictions. The international OPSC's scale is the widest as it states 'any representation, by whatever means' although most countries never criminalized all forms (Gillespie, 2016, p. 235). The other three instruments only consider the visual depictions of child sexual exploitation as child pornography. It is a logical choice if the justification for criminalization is based on the harm caused to children as it may cause secondary victimization through the later circulation of images (Taylor-Quayle, 2003, p. 194). Child pornography is not restricted to visual depiction but also can include text and audio depictions. Audio depictions can be just as harmful to children as images as these can be a recording of the sexual abuse of real children. Although it is not a common form of child pornography material, offenders may still find it sexually arousing (Gillespie, 2010, p. 214). Text-based material is the most problematic since if it does not include identifiable children it is much more in the 'fantasy' realm. The fact that these may have artistic value must be also considered, for example, Vladimir Nabokov's universally acclaimed novel *Lolita*.

Lastly, the nature of the material is to be addressed. There is a wide range of material from pictures that seem harmless in other contexts (e.g. catalog pictures of minors) to hardcore pornography. The UN Special Rapporteur in his report made a distinction between 'hardcore', 'softcore' and 'erotic' material. (Petit, 2004, p. 7-8) However, not all images will be subject to criminal law and thus there is a different categorization:

- Indicative: clothed children, implying a sexual interest in them,
- Indecent: naked children, implying a sexual interest in them,
- Obscene: children in explicit sexual acts.

Traditionally only the obscene images were punishable by criminal law (Gillespie, 2010, p. 206). In 2002, the University College Cork created the COPINE scale, which is a ten-point scale and it is used to categorize the level of seriousness of material with the aim to facilitate law enforcement cooperation (Astinova, 2013, p. 7). Three of the four international instruments (OPSC, Lanzarote Convention, Directive 2011/93) define the nature of the material as "a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes" while the Budapest Convention only contains the child engaging in sexually explicit conduct. The biggest problem with 'child erotica' (e.g. sexualized images of children in which the genitalia is covered) is that these can be freely disseminated and can undermine the effort to combat the sexual exploitation of children as a cover-up (Greijer & Doek, 2016, p. 42).

ICTS AND THE CHANGING PATTERNS OF CHILD PORNOGRAPHY

The use of ICTs changes the existing methods of creating and distributing child pornography. The ability to produce child pornography is greatly enhanced as digital images can be produced relatively cheaply without the need for external processing and reproduced with no diminution of quality. Cyberspace offers the opportunity to distribute the materials in large volumes, with minimal cost and relative anonymity (Clough, 2010, p. 249).

Virtual Child Pornography

As the production, possession, and distribution of child pornography is a serious offense in most countries, the perpetrators always try out new ways so that their activity falls into a gray zone of legality, which lowers the likeliness of persecution. It is much easier now, as technology has advanced to the point where a realistic depiction of a child can be created without a real child being involved (Gillespie, 2010, p. 211). The term 'virtual child pornography' in a wider sense refers to child pornography in cyberspace (including those with real children involved) while in a narrower, and more commonly used, sense it is pornography directly linked to cyberspace as it can only be produced in cyberspace (Poborilova, 2011, p. 242). There are three principal ways of creating virtual child pornography: 1) manipulating existing images (pseudo-photography) 2) computer-generating new images 3) dressing up adults as if they were minors (Gillespie, 2010, pp. 211-212).

Some authors use 'pseudo-photography' and virtual child pornography interchangeably (Gillespie, 2016, p. 245) but the latter term is wider and can include other forms of media like cartoons, manga, anime, etc. Pseudo-photography is created by digitally altering images, 'blending' or 'morphing' several together, for example putting a children's face on an adult's body to make it appear as if it is a child who is engaged in sexual activities (Greijer & Doek, 2016, p.41).

The main distinction Gillespie makes is that some images are only computer-manipulated while others are computer-created. Manipulating images can result in a new photograph that never actually took place (Gillespie, 2016, 245-246). Now even videos can be easily manipulated by the use of Deepfake, a technique for human image synthesis based on artificial intelligence, creating false images in only a few hours (Harris, 2019, p. 100). This can be utilized to produce child pornography and can be considered virtual child pornography. Computer-created images are fully generated by a computer and are not derivatives of photographs. It also must be noted that despite the rapid development of technology it appears that for the foreseeable future child pornography is likely to be created using real children (Clough, 2010, p. 272).

The main principle of virtual child pornography is that there is no abuse or other exploitation of a real child. As there are no children harmed during the production of these materials, the justification for criminalization must be on a different basis (Poborilova, 2011, p. 245). There are voices that claim private thoughts of an individual are part of the freedom of speech and criminalizing it would harm this principle (Gillespie, 2010, p. 213). The UK has put forward three principal justifications for criminalizing virtual child pornography: 1) it reinforces negative views toward children 2) it can be used for grooming children 3) it is frequently found alongside traditional child pornography. These justifications are rather weak: feeling in itself is rarely enough to justify criminalization (as freedom of speech extends to unpopular or offending opinions as well), many activities can benefit grooming unwillingly (more about that in the relevant chapter) and finally there are many things commonly found together with traditional child pornography (Gillespie, 2016, pp. 247-248). The US Supreme Court in the *Ashcroft v. Free Speech Coalition* concluded that prohibiting depictions of child pornography violated the First Amendment of the Constitution. The European Court of Human Rights in the case of *Karttunen v. Finland* in 2011 came to a different conclusion, stating that artists exercising freedom of expression are also subject to duties and responsibilities.

None of the international instruments contains a clear consensus in addressing the dilemma. The OPSC only refers to "child" and nothing indicates that this means anything other than a real child. The Budapest Convention's scope also extends to "a person appearing to be a minor engaged in sexually explicit conduct" and "realistic images representing a minor engaged in sexually explicit conduct" (Art 9. Para. 2). The Lanzarote Convention contains the definition of "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 purposes" (Art. 20. Para 2). This means that the two CoE instruments both persecute virtual child pornography but there is an 'opt-out' option for all signatory states. The EU Directive 2011/93 clearly covers all type of material and is legally binding for all EU member states.

Self-Generated Content, Sexting, and Sextortion

Another important problem that must be addressed is the question of self-generated content or self-exploitation. This phenomenon stems from increased access and exposure to pornography and the increased sexualization of children in the media (Leary, 2008, p. 18). It means that minors create images depicting themselves naked or during sexual acts and then send these to others. With the rise of the use of modern ICTs among minors (including computers with built-in web cameras and smartphones with quality cameras), it is becoming more common that they create and forward these materials among themselves.

This activity is often called "sexting" (Merriam-Webster, 2012) and there are even applications which encourage this behavior, like Snapchat. Adults can also engage in sexting between each other so in itself it is not a behavior that can be prohibited. According to research conducted in 2011, 1/3 of European children between the ages of 14-18 have had contact with sexting (Atabekova & Filippov, 2018, p. 765). 70% of 18-19 year-olds surveyed in one study felt pressure from another party to participate in sexting (Váradi-Csema, 2016, p. 642).

It can be as harmful as any other form of sexual exploitation for children. For example, in Denmark, there was a case where a sex video depicting a couple of 15-year-olds was shared by numerous people (mostly students) on the internet, a thousand of whom now face charges (Sorensen, 2018). Europol warns that such material, even if initially shared with innocent intent, often finds its way to "collectors", who often proceed to exploit the victim, in particular by means of extortion (Europol, 2018).

The law does not specify that child pornography must be created by others to be punishable which means that self-generated content is no exception from the law. Online predators can use it to blackmail children after they send them their first pictures and the scared minor is likely to continue sending more. This behavior is often called "sextortion". Addressing the problem, the CoE's Lanzarote Committee released their opinion in July 2019 (Lanzarote Committee, 2019). In their opinion, sexting by children should not be considered child pornography, when it is intended solely for their private use. And children coerced into such conduct should be addressed to victim support and not subjected to criminal prosecution.

Grooming

Grooming can be described as an act befriending minors and then inviting, inducing or coercing them into participating in or observing sexual acts and producing child pornography. Cyberspace facilitates this process in a way that communications can become intimate at a rapid speed (Clough, 2010, p. 332). Research shows that grooming is becoming less frequent as it requires a lot of time and effort to gain the trust of the victim. Now the period between initial engagement with a child and an offending outcome often can be extremely short (Greijer & Doek, 2016, p. 51).

According to a 2014 EU Survey, 20% of 14-16 years old children received sexual images online; 43% had contact online with someone they have not met face to face before, 11% sent their photo or video to these persons, and 14% met online contact offline (Atabekova & Filippov, 2018, p. 765). The Lanzarote Committee adopted an Opinion on the solicitation of children for sexual purposes through information and communication technologies (grooming) in 2015 (Lanzarote Committee, 2015). In this, it is stated that "the solicitation of children through information and communication technologies does not necessarily result in a meeting in person" (Art. 17). This means that grooming that only takes place in online space and does not include offline meetings can be as harmful as any other forms of grooming. Sexual offenses can be perpetrated online which leads to the production of child pornography.

Images of children engaged in sexual activity can be used as tools of grooming children for child pornography and sexual activity (Akdeniz, 2008, 22) and generated material, like the previously mentioned Deepfake videos can be used to encourage children to engage in sexual activity (Harris, 2019, p. 106). Seeing these, children might feel 'left out' and may be persuaded to participate actively in sexual activities (Váradi-Csema, 2016, p. 642).

According to O'Brien, there is a cycle of child pornography which first involves showing sexual material to a minor who is then convinced to participate in sexual acts which are filmed at a later stage, creating new material to attract other victims (Akdeniz, 2008, p. 5).

New Means of Distribution

The Budapest Convention requires parties to criminalize the distribution or transmission of child pornography through a computer system (Art. 9. (1)(c)). Although physical distribution was criminalized before the Convention, the increasing use of ICTs required this specification (Clough, 2010, p. 292). It is hard to decide what 'distribution" exactly means as it is undefined in international instruments or national legislations.

In 2006, it was estimated that there were more than 100,000 websites offering child pornography (Clough, 2010, p. 250). However, most of them are not on the surface web, which is well monitored. Dark Web plays a big role in distribution, which is accessible only through specialized applications, such as TOR (The Onion Router), where many criminal groups have been organized around the exchange and trade of child pornography content. Europol confirmed this in 2014, stating that the Darknets and other environments offering a high degree of anonymity are increasingly popular, especially among those with greater security awareness and IT knowledge. Such platforms host hidden services and marketplaces and are increasingly used by child sex offenders and producers (Jeney, 2015, p. 40). For example, the Lolita City community, the 1,500 members of which were eventually exposed by members of the Anonymous hacker group. The US-based pedophile group Candyman had about seven thousand members (Dornfeld & Mezei, 2017, p. 34).

The use of new technologies for distributing child pornography is becoming more regular. Two examples are peer-to-peer (P2P) or file-sharing networks and online streaming services. According to Europol, p2p networks are the main platform to access child abuse material and the principal means for non-commercial distribution. Meanwhile, online streaming means the profit-driven abuse of children overseas, the victims of which live in front of a camera at the request of Westerners (Europol, 2018).

The biggest problem in tackling streaming of material is that it is not covered in most of the international instruments as it is neither "acquisition" or "possession" of the illicit material. The Lanzarote Convention however criminalizes causing or coercing children to participate in child pornographic performances (Art. 21 (a)-(b)). However, it is only on the side of the perpetrator and as they are mostly located outside of Europe, often in Asia and Africa, therefore it is hard to prosecute them for these acts. Art. 24 criminalizes aiding or abetting such actions but it is questionable if simply watching a stream can be taken as such.

Anonymization and Encryption

The notion of anonymity is a very important factor for perpetrators when choosing to utilize the internet and ICTs. Two methods can achieve greater security for them in this regard: anonymization and encryption. While the first one aims at making communication more secure, the latter makes data accessible only to those who have the right encryption key to view it.

Anonymization devices include proxy servers and virtual private networks (VPNs), which allow users to easily obtain an IP address in any other country in the world. Another such tool is the TOR, developed by the United States for military purposes, which protects the content of communications using a hard-to-crack encryption method.

Until a few years ago, the use of steganography (hiding material in another, seemingly harmless file) was significant, but nowadays it is easy to filter out such files. Therefore, encryption programs, the effectiveness of which varies, are more commonly used now (Dornfeld & Mezei, 2016, 35). The nature of encrypted data remains unknown to the investigating authority and cannot be used as evidence. The question, therefore, arises as to whether the defendant may be required to provide the decryption key. In some member states, such as France, there is a provision in the Criminal Code (Art. 434-15-2), stating that the refusal to hand over the password or encryption key to the authorities is a criminal offense, while in Germany, for example, they intend to prevent this by using special police units and raids. In the United States, by contrast, such an obligation was found to be contrary to the prohibition of self-incrimination because the defendant effectively admits having unlawful information in the system.

Although detection is significantly more difficult if the offenders use for example proxy servers, passwords, encryption and/or steganography, according to a US study there are relatively few of them (20%) taking such steps. In addition, it must be noted that the survey was limited to those arrested so it might indicate that more people are actually applying the technology so successfully that they are virtually invisible to law enforcement (Clough, 2010, p. 250).

THE RESPONSE OF THE EUROPEAN UNION AND RECOMMENDATIONS

The European Union is involved in tackling online child pornography and other forms of sexual exploitation of children on many levels: policy, legal framework and institutional. The main legal instrument adopted was the Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography. Art. 3 of the Framework Decision requires the Member States to punish production, distribution, dissemination, transmission, acquisition or possession of child pornography and supplying or making available such material. Art. 8 (3) stated that if a Member State decides not to extradite its own citizen, it has to prosecute when the crime is committed by one of its own nationals outside its territory. Art. 8 (4) instructs Member States to ensure their jurisdiction in cases where the crime was committed by means of a computer system accessed from its territory, whether or not the computer system is in its territory.

In 2007, the European Commission reported that almost all of the Member States had ensured a high level of protection of children from sexual exploitation and abuse but there were problems not addressed by the existing legal regime (Jeney, 2015, p. 13). The Framework Decision proved to be inadequate for requiring proof of “explicit sexual conduct” but not abuse (Astinova, 2013, p. 27). In addition, in the three-pillar system of the EU, the Framework Decision was a rather weak form of secondary legislation, which suffered from many problems. It was similar in nature to Directives but unlike them, it had no direct effect and the transposition was not supervised, causing fragmentation (Dornfeld, 2016, p. 91). The EU’s previous legal regime regarding cybercrime (including online child pornography) was replaced both on a policy and on legislation level following the Treaty of Lisbon’s entry to force in 2009 (Buono, 2012, p. 332).

The first change was on a policy level. In 2009 in Prague at the Conference on ‘Safer Internet for Children - fighting together against illegal content and conduct on-line’ the ‘Prague Declaration’ was adopted. The Declaration is dedicated to the process of improving cooperation between all stakeholders in the field of promoting safer internet and mobile communications, especially for children (Buono, 2012, p. 337). There was a short-lived draft for a new Framework Decision on child pornography in 2009 (Herczeg, 2014, p. 71) but it was soon replaced by a new proposal for a Directive in 2010. This was adopted in 2011 as the Directive 2011/93, the content of which was addressed before in this chapter on multiple occasions.

The first articles of the Directive are about the definitions, the offenses, aggravating circumstances, etc. There were provisions regarding ICT-based child pornography, like criminalizing pornographic performance (Art. 4(3)), which means forcing a child to participate in pornographic performances (like the streaming mentioned before). Causing and recruiting a child for such performances and attending them was also criminalized. Solicitation for sexual purposes (grooming) is also a new offense in the Directive (Art. 6). Arts 12-13 contain provisions on the liability of legal persons and the relevant sanctions, which are standard regulations in all criminal Directives but here they seem out of place. Although legal persons can also benefit from child pornography (for example trading these materials), there is no precedence of companies engaging in such behavior.

The most interesting provision of the Directive is Art. 25 is titled 'Measures against websites containing or disseminating child pornography'. It also creates the opportunity for the Member States to create the legal basis for the prompt removal of web pages containing or disseminating child pornography hosted in their territory. If that is not possible, they can order internet service providers to block access to web pages containing or disseminating child pornography for Internet users within their territory. This is often called 'internet blocking' and is associated with authoritarian regimes like Russia, Turkey or China. The most serious problem with this solution is that, as it was presented in the chapter, the distribution of child pornography no longer takes place on the surface web. As other areas (like the deep web) is already hidden from the average user, the provision for internet blocking is redundant.

In the proposal of the Directive, the European Commission originally intended to impose a mandatory blocking obligation on the Member States if the effort to remove was unsuccessful. However, during the legislation process, concerns were raised like the potential breach of the right to freedom of expression, lack of adequate legal remedies against blocking measures, the inefficiency of blocking techniques considered easy to circumvent, potential censorship, "overblocking" (i.e. blocking of legal content), etc. So a compromise was reached, making this an optional measure for Member States (Jánoskúti, 2016, p. 74). The biggest fear was that if the states were bound to block the sites containing child pornography it would mean that computer systems and access to websites were to be monitored and confiscation of internet data without authorization could occur (Astinova, 2013, p. 32). In 2016, in total 13 Member States adopted regulation for blocking Internet sites. These are Belgium, Cyprus, France, Greece, Hungary, Italy, Lithuania, Luxembourg, Poland, Portugal, Romania, Spain and Sweden (Jánoskúti, 2016, p. 79). In Hungary, the system is not functioning well, as there were zero sites blocked for child pornography in 2016. Blocking is instead used as a tool to combat illegal online gambling and the selling of fake medicine (Dornfeld & Mezei, 2016, p. 35).

Useful tools for enforcing the provisions of the Directive are the EU's mutual recognition instruments, which abolish the double criminality requirement with respect to child pornography. Among others, this includes the European Arrest Warrant, the European Investigation Order and the Directive on Confiscation (Jeney, 2015, p. 20). However, these are mostly useful for gathering offline, physical evidence and not e-evidence. Addressing this problem, in 2019 the EU introduced its e-evidence proposal: A Directive and a Regulation. It introduces the "European Preservation Order" and the "European Production Order". The first one is about preserving data for later confiscation while the latter allows law enforcement to directly request electronic data from any service provider offering services in the EU, irrespective of where the provider's headquarters are located or where the respective data is stored physically. This is a very big step forward for European legislation.

On a policy level, the EU has adopted the Digital Agenda for Europe as one of the pillars of the Europe 2020 Strategy. As a part of achieving these goals, the European Commission drafted a ‘Strategy for a Better Internet for Children’, which proposed a series of actions to be undertaken by the European Commission, EU Member States and by the ICT industry (Jeney, 2015, p. 23). Victim identification is an important step in tracking down online child pornography, preventing victimization and stopping the further spread of damaging material. Interpol, for example, created an international image database on child sexual exploitation in 2009, providing real-time access to the collected footage, and its February 2016 version provides the ability to analyze video footage (Dornfeld & Mezei, 2017, p. 34). This approach should be strengthened in the EU as well. There is no obligation for the Member States to introduce the registration of sex offenders, as they have the option not to create such a register and there is no European level equivalent either. This means that offenders can easily avoid professional disqualification by cross-border movement, which is unimpaired in the European Union (Jeney, 2015, pp. 42-43).

There were changes in the institutional framework as well. The biggest of those is the establishment of the European Cybercrime Centre (EC3) as a part of Europol. As the Europol has no legal basis to conduct investigations directly, its main goal is to coordinate the work of the Member States’ law enforcement agencies. EC3, in particular, focuses on the fight against online crime that causes serious harm to the victim, including sexual exploitation of children and child pornography. According to a report on the first year of organization, the center was involved in nine large-scale operations against child sexual abuse in 2013 (Dornfeld & Mezei, 2016, 36). Working alongside EC3 is the Joint Cybercrime Action Taskforce (J-CAT), which works on the most important international cybercrime cases, including online sexual exploitation of children that affect the EU Member States and their citizens.

FUTURE RESEARCH DIRECTIONS

There are many topics not addressed in detail in this chapter that are open to future research. One of those is the question of jurisdiction, as the problem of child pornography is a global one, while the legislation response is mainly on a national level. The topic of criminal cooperation is also an interesting one, as there are many cross-border cases and the tools at the disposal of law enforcement are mostly outdated. Legal and investigational responses to the threat of anonymization and encryption is also a hotly debated and interesting topic to research. Victimology and the criminological aspects of increasing youth indecent communication can be potential future areas of research as well.

CONCLUSION

As the chapter shows, online child pornography is a highly complex social phenomenon that targets the most vulnerable in society and recently became an even larger threat due to the rapid development of ICTs. From the start, there are many controversial topics, including the proper term for the phenomenon. One cannot find a settled agreement on the definition, which is not an entirely academic question, as it raises practical issues as well. For example, double criminality is required for law enforcement to request mutual legal assistance from other agencies abroad. There is no unified approach to define child pornography and more harmonization is required on both international and regional level.

The methods of committing the crime are rapidly evolving due to new ICTs. It is hard for legislation and law enforcement to keep up with these new developments. Streaming is currently only punishable on the creator's side, not the consumer's. File-sharing, deep web groups and other places provide the suitable environment for perpetrators to engage in trading and exchanging these materials. They cover up their tracks and hide evidence using other technologies, such as anonymization and encryption. However, the problem is not entirely technological but also social in nature. Minors use technology to shape their personalities and often engage in indecent communication like sexting, which can be used by predators to coerce them into participating in future child pornographic materials (grooming, sexting). A "cycle" of child pornography can be found.

EU's current legislation, policy and institutional framework is quite effective. However, there are some problems as well, like the utilization of the ineffective tool of internet blocking, the lack of EU-level registration of sex offenders and the lack of engagement in identifying victims. These questions have to be addressed in the future to provide an even better protection on a regional level. The other big problem, however, is much harder to deal with. As online child pornography is a global phenomenon, perpetrators can easily hide outside the EU, like in East and South Asia. A global approach and cooperation is a very important issue for the future.

REFERENCES

Aiken, M., Moran, M., & Berry, M. J. (2011). *Child abuse material and the Internet: Cyberpsychology of online child related sex offending*. Paper presented at the 29th Meeting of the INTERPOL Specialist Group on Crimes against Children, Lyons, France.

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

Astinova, M. (2013). *The Crime of Child Pornography: European Legislative and Police Cooperation Initiatives* (Master Thesis). Tilburg University.

Atabekova, A., & Filippov, V. (2018). Legislation Response to Use of Minors' Self-generated Sexual Content for their ICT-facilitated Sexual Coercion. *European Research Studies Journal*, *21*(4), 763–772.

Buono, L. (2012). Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). *New Journal of European Criminal Law*, *4*(3), 332–343. doi:10.1177/203228441200300307

Clough, J. (2010). *Principles of Cybercrime*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511845123

Dornfeld, L. (2016). A kiberbűncselekmények nyomozásával kapcsolatban folytatott uniós bűnügyi együttműködés fejlődése. *Külügyi Szemle*, *15*(4), 89–101.

Dornfeld, L., & Mezei, K. (2017). Az online gyermekpornográfia elleni küzdelem aktuális kérdései. *Infokommunikáció és Jog, 14*(68), 32–37.

Europol. (2018). *Child sexual exploitation*. Retrieved from: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation

Gillespie, A. A. (2010). Defining Child Pornography: Challenges for the Law. *Child and Family Law Quarterly*, *22*(2), 200–222.

Gillespie, A. A. (2012). *Child pornography: Law and policy*. New York, NY: Routledge. doi:10.4324/9780203818107

Gillespie, A. A. (2016). *Cybercrime: Key issues and debates*. New York, NY: Routledge.

Greijer, S., & Doek, J. (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. Luxembourg: ECPAT.

Harris, D. (2019). Deepfakes: False Pornography Is Here and the Law Cannot Protect You. *Duke Law & Technology Review*, *17*, 99–128.

Herczeg, J. (2014). Actual problems of possession and viewing child pornography in Internet. *Jura*, *20*(1), 70–80.

Jánoskúti, B. (2016). Take down and blocking measures (Art. 25 & recitals 46-47). In *Survey on the transposition of Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography*. Retrieved from: http://missingchildreneurope.eu/Portals/0/Docs/A%20survey%20on%20transposition%20of%20Directive%20against%20child%20sexual%20exploitation%20and%20abuse.pdf

Jeney, P. (2015). *Combatting child sexual abuse online*. Study for the LIBE Committee. Retrieved from: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536481/IPOL_STU(2015)536481_EN.pdf

Lanzarote Committee. (2015). *Opinion on Article 23 of the Lanzarote Convention and its explanatory note. Solicitation of children for sexual purposes through information and communication technologies (Grooming)*. Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064de98

Lanzarote Committee. (2019). *Opinion of the Lanzarote Committee on child sexually suggestive or explicit images and/or videos generated, shared and received by children*. Retrieved from: https://rm.coe.int/opinion-of-the-lanzarote-committee-on-child-sexually-suggestive-or-exp/168094e72c

Leary, M. G. (2008). Self-Produced Child Pornography: The Appropriate Societal Response to Juvenile Self-Sexual Exploitation. *Virginia Journal of Social Policy & the Law*, *15*(1), 1–50.

Mathew, L. A. (2009). Online Child Safety from Sexual Abuse in India. *Journal of Information Law & Technology, 1*. Retrieved from: https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/mathew

Merriam-Webster. (2008). *Sexting*. Retrieved from: https://www.merriam-webster.com/dictionary/sexting

Partner S. P. E. A. K. (2015). *Online child abuse material is not 'child pornography'*. Retrieved from: http://www.partnerspeak.org.au/articles/online-child-abuse-material-is-not-pornography

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

Poborliova, M. (2011). Virtual Child Pornography. *Masaryk University Journal of Law and Technology*, *5*(2), 241–253.

Quayle, E. (2011). Child pornography. In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 343–368). Devon, UK: Willan Publishing.

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

Taylor, M., & Quayle, E. (2003). Child Pornography. An Internet Crime. Brunner-Routledge.

Váradi-Csema, E. (2013). Gyermek- és fiatalkori bűnözés alapkérdései, különös tekintettel a serdülőkor pszichés sajátosságaira. In Á. Farkas (Ed.), *Tanulmányok a bűnügyi tudományok köréből* (pp. 5–42). Miskolc, Hungary: Gazdász Elasztik.

Váradi-Csema, E. (2016). A gyermek- és fiatalkori kriminalitás. In A. Borbíró, K. Gönczöl, K. Kerezsi, & M. Lévay (Eds.), *Kriminológia* (pp. 616–651). Budapest, Hungary: Wolters Kluwer.

ADDITIONAL READING

Calcara, G. (2013). Role of INTERPOL and Europol in the Fight against Cybercrime, with Particular Reference to the Sexual Exploitation of Children Online and Child Pornography. *Masaryk University Journal of Law and Technology*, *7*(1), 19–33.

Chawki, M. (2009). Online Child Sexual Abuse: The French Response. *Journal of Digital Forensics. Security and Law*, *4*(4), 7–42.

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Switzerland: Springer. doi:10.1007/978-3-319-15150-2

Döring, N. M. (2012). Internet Sexuality. In Z. Yan (Ed.), *Encyclopedia of Cyber Behavior* (pp. 808–827). IGI Global. doi:10.4018/978-1-4666-0315-8.ch067

Gillespie, A. A. (2012). Jurisdictional issues concerning online child pornography. *International Journal of Law and Information Technology*, *20*(3), 151–177. doi:10.1093/ijlit/eas007

McIntyre, T. J. (2010). Blocking Child Pornography on the Internet: European Union Developments. *International Review of Law Computers & Technology*, *24*(3), 209–221. doi:10.1080/13600869.2010.522321

Parti, K. (2009). Online child pornography in Hungary - analysis of research findings. *Studia Iuridica Auctoritate Universitatis Pecs Publicata*, *144*, 247–265.

KEY TERMS AND DEFINITIONS

Anonymization: A process of destroying online tracks of the data that could be used to link it to its originator.

Encryption: The process of encoding a message or information in such a way that only authorized parties can access it.

Grooming: The solicitation of children for sexual purposes.

Internet Blocking: Blocking access for users to certain Internet sites on a national level.

Sexting: A common practice among young persons, which involves taking sexually explicit images of one's self and sending it to others via ICTs.

Sextortion: A form of sexual exploitation during which the victim is coerced to provide sexual favors (including child pornography material) to the perpetrator.

Virtual Child Pornography: Child pornography produced by digitally modifying pre-existing images or fully generated by a computer.