The Evolution of Content-Related Offences and Their Investigation During the First 20 Years of the Cybercrime Convention

Kinga Sorbán[*]

Abstract

The Convention on Cybercrime otherwise known as the Budapest Convention was a complex, pioneering instrument addressing cross-border computer crimes in the wake of the 21st century. As the first international treaty aiming to tackle new threats emerging from the cyberspace, the Convention signed in 2001 certainly influenced national regulators and law enforcement over many years. Two decades have passed since 2001 and the Internet era has undergone previously unpredictable changes, as web 2.0 services started to thrive. Even though the Convention can be considered a landmark in international legislation, after 20 years one must eventually assess how well it stood the test of time and whether it still has relevance. This article has no smaller goal but to evaluate the evolution of content-related cybercrimes and try to the question whether the Convention is still fit to tackle contemporary issues or rather, is outdated and ready to retire.

Keywords: cybercrime, content-related offence, cyberbullying, privacy, wiretapping.

1. Introduction

The Convention on Cybercrime otherwise known as the Budapest Convention was a complex, pioneering instrument addressing cross-border computer crimes in the wake of the 21st century. As the first international treaty aiming to tackle new threats that emerged from cyberspace, the convention signed in 2001[1] certainly influenced national regulators and law enforcement over many years. 20 years have passed since 2001 and the Internet era has undergone under previously unpredictable changes, as web 2.0 services started to thrive. Web 2.0 was described as an embryo in development by Darcy DiNucci in 1999[2] who envisioned that instead of remaining a static collection of texts and images the

* Kinga Sorbán: junior research fellow, National University of Public Service, Budapest.

1 The Convention was signed on 23 November 2001 and is in force from 1 July 2004.

2 Cristina Aced, *Web 2.0: The Origin of the Word that Has Changed the Way We Understand Public Relations*', International PR 2013 Conference.

doi: 10.5553/HYIEL/266627012021009001017

Internet will be a "transport mechanism, the ether through which interactivity happens."[3]

A couple of years after the signatories adopted the Cybercrime Convention, web 2.0 services started to spread and now we live in an era of abundance in terms of web-based interactive services. There were 361 million Internet users in 2000, now that accounts for two-thirds of the clients of Facebook.[4] The first camera phones appeared around 2000, although around the time the Convention was drafted, it was a high-tech gadget only available to a select few. In our present days, almost everybody has a smartphone or tablet in their bag, with broadband internet access. Facebook was founded in 2004, now it is a social media platform that is among the most important drivers of societal discourse. The notable service YouTube was launched in 2005 when founding member Jawed Karim uploaded his first video entitled "Me in the Zoo".[5] After Google acquired this media service provider in 2006[6] it became the largest global video-sharing platform, with 500 hours of videos being uploaded every minute.[7] Our present days' largest microblogging platform Twitter was launched in 2006. Since then, it has gathered more than 100 million users,[8] among them, politicians and heads of states informing the public.[9]

The Convention received harsh criticism from the very beginning. Jason Wallace for example argued that its wording was too vague, claiming it would trammel civil rights and privacy.[10] Arguing against its signature, Ryan M.F. Baron considered it more of a liability than an asset, raising several concerns including the lack of specific protection for privacy rights[11] and the absence of proper procedural safeguards which allow countries to "use the treaty as a means to enforce government policies".[12] Despite all the criticism it was signed and ratified, and for a long time it remained the sole and most important international tool to tackle computer crime. Several regional and national instruments drew on the Convention, and it also had an impact on the law of the

3 Darcy DiNucci, 'Fragmented Future', *Print Magazine*, Vol. 53, Issue 4, 1999, p. 32, at http://darcyd.com/fragmented_future.pdf.

4 *See* at www.pingdom.com/blog/incredible-growth-of-the-internet-since-2000/#:~:text=There%20were%20only%20361%20million,2000%2C%20in%20the%20entire%20world.

5 Kevin Allocca, *Videocracy*. Bloomsbury, 2018.

6 Andrew Ross Sorkin & Jeremy W. Peters, 'Google to Acquire YouTube for $1.65 Billion', *The New York Times*, 9 October 2006.

7 Hours of Video Uploaded to YouTube Every Minute as of May 2019, at www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/.

8 Number of monetizable daily active Twitter users (mDAU) worldwide from 1st quarter 2017 to 1st quarter 2021, at www.statista.com/statistics/970920/monetizable-daily-active-twitter-users-worldwide/.

9 *See e.g.* the Twitter account of US President Joe Biden at https://twitter.com/JoeBiden, or of European Commission President Ursula von der Leyen, at https://twitter.com/vonderleyen.

10 Jason Wallace, *Council of Europe Cybercrime Treaty Analysis*, at www.ithell.com/Opinion/CybercrimeTreaty/body-cybercrime-treaty.html.

11 Ryan M.F. Baron, 'A Critique of the International Cybercrime Treaty', *CommLaw Conspectus: Journal of Communications Law and Technology Policy*, Vol. 10, Issue 2, 2002, p. 278.

12 Id. p. 275 and 278.

doi: 10.5553/HYIEL/266627012021009001017

EU, as the instruments of European cybercrime legislation were worded in accordance with the Cybercrime Convention.

Even though the Convention may be considered a landmark in international legislation, after 20 years one must eventually assess how well it stood the test of time and whether it still has relevance. This article has no smaller goal but to *evaluate the evolution of content-related cybercrimes and try to the question whether the Convention is still fit to tackle contemporary issues or rather, is outdated and ready to retire*. I will proceed in this evaluation by examining the following four key areas of the Convention. *(i)* First, the article will take a look at the Convention's overall structure giving a detailed description of its categorization of cybercrime. This first Section also serves the purpose of determining how content-related cybercrimes fit into the framework established by the Cybercrime Convention. *(ii)* Second, the wording of the Convention will be compared to newly emerged definitions describing the same or similar content-related conducts criminalized. *(iii)* Third, emerging cybercrime trends will be described along with an assessment of whether these new trends fall under the crime categories regulated by the Convention. *(iv)* Last but not least the article will elaborate on the procedural provisions of the Cybercrime Convention that enable the collection of electronic evidence in the online sphere. The Section will articulate concerns that were raised regarding the constitutionality of these procedural provisions putting an emphasis on privacy-based concerns. The final Section of this article makes an attempt to predict the future of cybercrime legislation. In this section I try to describe how the 2nd Additional Protocol to the Convention will affect the current state of play, furthermore, I will formulate some critical remarks with the aim to contribute to scientific and regulatory discourse about cybercrime legislation.

2. The Structure of the Cybercrime Convention

The Convention is a multi-purpose treaty containing substantive criminal law provisions, procedural provisions and elements concerning cross-border procedures, regulating the determination of jurisdiction, and international cooperation. The aim of the Cybercrime Convention is to approximate the State Parties' legal systems in the area of combatting cybercrime. Prior to getting into the assessment of the provisions on content-related crimes it is worth outlining what is meant by cybercrime in general.

2.1. Cybercrime

Despite the fact that cybercrime is a term that appears in the title of the Convention itself, the *notion of cybercrime is not defined nor used in the text*. Instead, many other terms appear in the text to describe information technology-related criminality, such as crimes against the confidentiality of computer systems, computer-related offence and content-related offence. One must therefore first determine whether there is a difference between the concepts of cybercrime, computer crime and computer-related crimes or whether these are

interchangeable notions. A publication by the International Telecommunications Union (ITU) argues that these terms cover different concepts, and that 'cybercrime' is a narrower concept than computer crime.[13] It notes that there are considerable difficulties in creating distinctive definitions as there is an abundance of regional and national approaches.

Delving into the scholarly literature on the subject does not alleviate the confusion generated by the diversity of terms. Eoghan Casey refers to computer crime as a limited set of offences that involve a computer such as unauthorized access and software piracy, while defining computer-related crimes as offences that involve a computer indirectly (*e.g.* when evidence can be gathered from a computer).[14] Cybercrime is used by Eoghan Casey as a term to describe offences where a computer network was used to facilitate the offence.[15] A similar definition is applied by Joshua B. Hill and Nancy E. Marion, who refer to cybercrime as acts "that involve criminal uses of the Internet or other networked systems to cause harm".[16] The abovementioned ITU publication shares this concept and covers any illegal behavior committed by means of, or in relation to a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.[17] In its communication the European Commission defines cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems".[18]

According to Susan W. Brenner the term cybercrime refers to a broader set of offences and includes all kinds of criminal acts that involve information technology.[19] Brenner splits the notion into three subcategories based on the role of the computer in the commission of the act. Target cybercrimes refer to a narrow set of acts where the computer is the object of the crime (such as hacking or malware distribution) while tool cybercrimes include those crimes where the computer or the network is the tool used to commit the crime.[20] I prefer the first approach and consider *cybercrimes to be network-related crimes*. Cybercrimes can be computer crimes (or target crimes) and computer-related crimes (tool crimes) alike if the commission involves a network (either the Internet or a LAN). However, interpreting cybercrime in a narrower sense may not have been the intention of the drafters of the Cybercrime Convention, because adopting this approach would mean that offences without a network element (*e.g.* hacking into a system onsite) are not covered.

13 Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, 2012, p. 11.
14 Eoghan Casey, *Digital Evidence and Computer Crime, Third Edition*, Elsevier, 2011, p. 37.
15 Id. p. 37.
16 Joshua B. Hill & Nancy E. Marion, *Introduction to Cybercrime. Computer Crimes, Laws, and Policing in the 21st Century*, Praeger, 2016, p.10.
17 Gercke 2012, p. 11.
18 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, *Towards A General Policy on the Fight against Cyber Crime*, COM(2007) 267 final.
19 Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, Praeger, 2010, p. 39.
20 Id.

doi: 10.5553/HYIEL/266627012021009001017

Despite its widespread use, *cybercrime is not a legally defined term*, as it does not appear in regulatory instruments. Legislators often adopt a typology-related approach to describe what kinds of acts fall under the notion of cybercrime, which is flawed, because there are significant overlaps between the categories. The Cybercrime Convention also adopted a typology-related approach which will be discussed in more detail in the following Section.

2.2. Substantive Provisions of the Cybercrime Convention

According to the Explanatory Report of the Convention,[21] Chapter II which covers substantive criminal issues defines 9 offences grouped into 4 categories. The four categories are the following: *(i)* traditional computer crimes which cover offences against the confidentiality, integrity and availability of computer data and systems, such as illegal access (hacking), data and system interference (malware distribution, DDOS attacks);[22] *(ii)* computer-related offences, such as computer-enabled forgery and fraud;[23] *(iii)* content-related offences;[24] and *(iv)* offences related to infringements of copyright.[25]

The Explanatory Report describes *computer-related offences as ordinary crimes committed through a computer system*[26] and lacks a definition for content-related crimes. This approach may cause problems, because sometimes it is not easy to make clear distinctions between computer-related offences and content-related offences. In fact, content-related offenses are a sub-category of computer-related offences, because acts related to unlawful material in a networked environment always include the use of information technology as a tool.

2.3. Content-Related Offences

The fact that the Cybercrime Convention does not define this term results in a conundrum for all those wishing to identify what acts shall be considered content-related offences. Under the title content-related offences, the Convention regulates only offences related to child sexual abuse material causing a conundrum for researchers, policy analysts and regulators. It is evident that activities concerning child sexual abuse material[27] are indeed content-related offences but it is also clear that the list of content-related offences cannot be narrowed down to simply these activities. The Additional Protocol to the Convention[28] criminalizes the dissemination of racist and xenophobic content on the Internet [such as the dissemination of such material on computer systems

21 Explanatory Report to the Convention on Cybercrime (Explanatory Report), para. 18.
22 Cybercrime Convention, Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems
23 Id. Title 2 – Computer-related offences.
24 Id. Title 3 – Content-related offences.
25 Id. Title 4 – Offences related to infringements of copyright and related rights.
26 Explanatory Report, para. 79.
27 Though the text of the Convention refers to child pornography this term is now outdated as is not capable to reflect the seriousness of the offences. The article therefore will refer to child pornography as child sexual abuse material.
28 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189.

(classic hate speech), bias-motivated threats, insults, and the denial, gross minimization, approval or justification of genocide or crimes against humanity], expanding the list of content-related offences. Yet even with the Additional Protocol, *the Convention does not cover the full scale of content-related offences*. Three reasons may be identified to justify these deficits of the Convention. *(i)* The first and evident reason is that the drafters of the Convention never strived for completeness, even the Explanatory Report notes, that the Convention was created to set the foundation for the harmonization of cybercrime-legislation and offers only a minimum level of protection. Thus, State Parties are only obliged to criminalize those core offences that are regulated by the Convention, while they are not excluded from adopting a stricter and more detailed regime to tackle cybercrime in their countries. *(ii)* Second, there are some new and malicious activities on the Internet that cannot be regulated globally or regionally. While there is a broad worldwide consensus behind the criminalization of serious acts (*e.g.* the acts related to the creation and dissemination of child sexual abuse material), such a common understanding is missing in the case of several forms of objectionable content. For example: some types of communication amount to criminal offences in certain countries, while they are considered to be protected speech in other countries as they fall under the umbrella of freedom of speech. This is the case with defamation which is punishable in Hungary[29] while criminal defamation was abolished in the United Kingdom by Section 73 of the Coroners and Justice Act 2009. Cultural, social, and governmental specificities can influence whether a certain act is considered punishable by criminal law and since criminal legislation is within the inner core of national sovereignty, it is not easy to develop criminal law on a supranational level. In Europe, the EU never fully harmonized Member State's criminal laws. There are areas where criminal laws were approximated in order to achieve certain policy objectives, mainly for the sake of ensuring the cross-border collection of evidence, to guarantee fair trial[30] and to tackle criminal acts that have cross-border elements,[31] or directly target the institutions of the EU.[32] *(iii)* The third reason is that the Convention was

29 Act C of 2012 on the Criminal Code, Section 226.

30 *See e.g.* Directive 2010/64/EU of the European Parliament and of the Council on the right to interpretation and translation in criminal proceedings; Directive 2012/13/EU of the European Parliament and of the Council on the right to information in criminal proceedings; Directive (EU) 2016/343 of the European Parliament and of the Council on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings.

31 *See e.g.* Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA; 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, and replacing Council Framework Decision 2004/68/JHA; Directive (EU) 2017/541 of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

32 *See e.g.* Convention drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union.

doi: 10.5553/HYIEL/266627012021009001017

adopted in the early 2000s.[33] The drafters could not anticipate all the remarkable achievements that influenced the online industry. We use the Internet to communicate and share content in a way that probably no one could predict. While many people use online communication for working or to stay in touch with friends and family members, some have malicious intent and aim to cause harm. As offenders started to rely on new technologies, the crimes that were originally committed in the physical world such as non-content related crimes (like harassment, stalking or fraud) and content-related crimes (like hate speech and incitement to terrorism) oozed into the virtual space.[34] Besides the evolution of traditional crimes committed in the virtual world, some unforeseen yet harmful conducts gained unprecedented popularity, including image-based abuse (such as revenge pornography) and bullying.

At this point, one may come to the conclusion that it is not possible to formulate an exhaustive list of content-related offences. However, coining a definition and establishing a uniform terminology would be welcomed as it would enable State Parties to draw up their lists of content-related offences on a common foundation. This article considers those acts to be *content-related offences, where a computer or a network is used as a tool to produce, distribute, transmit, procure, possess or store illegal content*. The list of illegal content shall include those materials that are criminalized by international law (such as the Cybercrime Convention) and those materials that are unlawful under national jurisdictions. Although it would be favorable to expand and change the terminology by amending the Convention in order to maintain the clarity of the text, it is not necessary. The Convention has an Explanatory Report and several guidelines which serve the purpose of clarifying certain provisions.

The article has two objectives concerning content-related cybercrimes. *(i)* First, it will introduce how those types of content-related crimes changed which are already criminalized by the Convention. This part of the article will carefully evaluate whether these crimes are sufficiently regulated and will explore the extent to which the current regulatory framework is efficient to tackle these offences. *(ii)* Second, the article will draw attention to newly emerged phenomena, which pose an issue for regulators but are not yet covered by the Convention. Prior to unfolding the previously highlighted issues, one must add, that the Convention shall not be considered a standalone legal instrument. On the contrary, it is but a piece in a very complex system of legislative instruments regulating the cybercrime landscape and should be seen as part of a bigger picture. In order to illustrate the Convention's position within the regulatory landscape, the article will draw up the comprehensive regulatory framework of all

33 The Convention was signed on 23 November 2001 and entered into force on 1 July 2004.

34 Statista reported a significant increase in cyber fraud risk due to the COVID-19 pandemic, at www.statista.com/statistics/1175574/increase-cyber-fraud-coronavirus-outbreak/. The Pew Research Center's survey conducted in the US revealed that roughly four-in-ten Americans have experienced online harassment, *see* at www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/. In the UK, 2% of adult hate crimes have an online element, *see* at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf.

the conducts discussed, elaborating on the most important conventions and supranational legal instruments complementing the Cybercrime Convention.

3. Content-Related Offences in the Cybercrime Convention

According to its Explanatory Report, the language of the Cybercrime Convention was chosen to be technologically neutral in order to futureproof the text.[35] This futureproofing however could not prevent changes to certain notions. The following Section will elaborate on the terms currently used by the Cybercrime Convention and introduce alternatives where it is necessary to update the Convention's wording to keep it relevant.

3.1. Child Sexual Abuse Material

According to the Cybercrime Convention, producing, offering, making available, distributing, transmitting, procuring, and possessing child pornography shall constitute a criminal offence. The Convention consistently uses the term child pornography for child sexual abuse material for which it has received severe criticism. The Convention defines child pornography as

> "pornographic material that visually depicts: *(a)* a minor engaged in sexually explicit conduct; *(b)* a person appearing to be a minor engaged in sexually explicit conduct; *(c)* realistic images representing a minor engaged in sexually explicit conduct."[36]

The Lanzarote Convention on the sexual exploitation of children[37] echoes the criminalization of offences related to child sexual abuse material. The Lanzarote Convention (which also uses the term child pornography) defines the term as follows:

> "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 purposes."[38]

Several differences can be spotted between the two definitions. First and foremost, the Lanzarote Convention *uses the term 'child' instead of minor*. Furthermore, the Lanzarote Convention only aims to criminalize offences that victimize real children: virtual child pornography and the conduct of adult actors mimicking minors are not addressed, while the Cybercrime Convention also covers material that depicts persons representing or appearing to be minors. As such the two Conventions establish different levels of protection: those States

35 Explanatory Report, para. 36.
36 Cybercrime Convention, Article 9 – Offences related to child pornography.
37 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.
38 Lanzarote Convention, Article 20 – Offences concerning child pornography.

doi: 10.5553/HYIEL/266627012021009001017

that did not sign and ratify the Cybercrime Convention have to criminalize a narrower set of conducts. The different levels of protection give rise to merely theoretical debates and do not pose a problem in practice, because the Cybercrime Convention was signed and ratified by all State Parties of the Lanzarote Convention.[39]

Both definitions have *two troublesome elements: the definition of pornographic material and the definition of a minor*.

3.1.1. Sexual Abuse and Pornography

Using the term pornography for describing acts related to the sexual exploitation of children is deemed to be controversial by many, including Allisdair Gillespie as it underplays the significance of the issue.[40] The dictionary definition of pornography states that pornography "is the depiction of erotic behavior (in pictures or writing) intended to cause sexual excitement."[41] Edwards argues that child sexual abuse material cannot be considered erotica as this imagery represent the "rape, abuse and torture of children".[42] The Luxemburg Guidelines on terminology highlights that the term pornography is generally used to describe a commercial product in which consenting adults engage in sexual activity.[43] Danijela Frangež *et al*. highlight that pornography is a commonly used term, which is broadly accepted, trivialized and refers to a type of material that is legal in the majority of the countries of the globe and using the term for material depicting the sexual abuse and exploitation of children may, in fact, legitimize the phenomena.[44]

Adolescents engaging in sexual activities may encounter several new online behaviors that gained popularity since the Convention was adopted. Sexting, meaning the creation and distribution of sexually explicit imagery by text messages or social media have gained popularity among young people in the last couple of years.[45] It would seem illogical and unnecessary to charge teenagers with the creation and dissemination of 'child pornography' yet the Convention does not make a distinction between different kinds of sexual imagery involving

39 *See* the Chart of signatures and ratifications of the Cybercrime Convention at www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Ie8q5VWb; and the Chart of signatures and ratifications of the Lanzarote Convention at www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/signatures.

40 Alisdair A. Gillespie, 'Child Pornography', *Information & Communications Technology Law*, Vol. 27, Issue 1, 2018, p. 31.

41 Merriam-Webster, *Definition of Pornography*, at www.merriam-webster.com/dictionary/pornography.

42 Susan S. M. Edwards, 'Prosecuting 'Child Pornography': Possession and Taking of Indecent Photographs of Children', *Journal of Social Welfare and Family Law*, Vol. 22, Issue 1, 2000, p. 1.

43 Susanna Greijer & Jaap Doek, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, ECPAT International, Bangkok, 2016, p. 38.

44 Danijela Frangež *et al*., 'The Importance of Terminology Related to Child Sexual Exploitation', *Journal of Criminal Investigation and Criminology*, Vol. 66, Issue 4, 2015, pp. 291-299.

45 Bruce Y. Lee, 'Here Is How Much Sexting Among Teens Has Increased', *Forbes*, 8 September 2018, at www.forbes.com/sites/brucelee/2018/09/08/here-is-how-much-sexting-among-teens-has-increased/?sh=2dfcb4be36f1.

children. It has to be noted that it is not the aim of criminal law to hold persons accountable for conduct that poses little to no danger to society or its members, so to alleviate the concern, a more nuanced wording should be adopted.

A commonly used term in our present days is *child sexual abuse material (CSAM) and child sexual exploitation material (CSEM)*. The latter is used by international police organizations such as Europol,[46] while the former is used by several organizations and private entities including the International Association of Internet Hotlines (INHOPE)[47] and YouTube (Google). The EU also uses the term child pornography, but its Directive on combating the sexual abuse of children clarifies that child pornography consists of images of child sexual abuse.[48] The EU also acknowledged the inadequacy of the term child pornography. The European Parliament started communicating its effort to correct the terminology in its Resolution on Online Child Sexual Abuse in 2015.[49] Either of these terms is acceptable, because they clearly indicate that we are in fact talking of violent, abusive conduct that takes places on a regular basis often with the aim of realizing financial gain. These terms do not cover self-generated, sexually explicit content produced consensually (unless consent is a result of putting pressure on, or coercing children) which helps avoid an unnecessary stigmatization of adolescents.

3.1.2. Minor

While the Cybercrime Convention refers to child sexual abuse material as child pornography, it does not define who should be regarded as a child, instead, it uses the term 'minor'. According to the Cybercrime Convention, *the term minor shall refer to persons under 18 years of age, but State Parties are free to set a lower age limit (but not less than 16 years of age)*.[50] This definition is in accordance with the UN Convention on the Rights of the Child, which uses the same definition, but refers to children. While the two terms appear to be synonymous they are not. The term 'child' shall be perceived as a universal term, referring to all persons under the age of 18 years, while the term 'minor' should be understood as a legal notion. The Luxemburg Guidelines describe minors as persons who have not reached the age of majority.[51] The age of majority is "is the legally defined age at which a person becomes an adult, with all the attendant rights and responsibilities of adulthood."[52] The age of majority is generally set at 18 years, but some exceptions exist. Under some jurisdictions, persons under 18 can become emancipated (*e.g.* by marriage or by obtaining a court order) which means that children can legally

46 *See* at www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation.
47 *See* at www.inhope.org/EN.
48 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, and replacing Council Framework Decision 2004/68/JHA, Recital (3).
49 European Parliament Resolution of 11 March 2015 on child sexual abuse online, 2015/2564(RSP), para. 12.
50 Cybercrime Convention, Article 9(3).
51 Greijer & Doek 2016, p. 8.
52 Id. p. 6.

doi: 10.5553/HYIEL/266627012021009001017

attain the status of adults. It is generally presumed that minors cannot legally consent to the creation of pornographic material,[53] since they lack sufficient discretion to assess the consequences of their actions. However, the status of being an emancipated minor expressly involves the capability to make certain decisions (such as entering into contracts or managing property) on their own behalf. In the case of emancipated minors, there is clearly a tension between the legal status of a person and the protection offered by the Cybercrime Convention. Being an emancipated minor shall not result in certain persons between the ages of 16 and 18 losing their status as a child and becoming excluded from the protection that international legal instruments provide to children. Thus, it would be strongly recommended for the Cybercrime Convention to use the term 'child' which generally refers to any person under the age of 18 regardless of the legal status. The EU Directive on combating the sexual abuse of children defines and uses the term 'child' and considers any person below the age of 18 years to be a child.[54]

The age-based approach of the Cybercrime Convention may also be challenged. László Dornfeld notes that the biggest problem of the age-based approach is that there is a gap between the age of consent and the protection offered by laws aiming to protect children.[55] The age of consent is 16 years old in the UK, 14 in Germany if both partners are under 18, 15 in France, 12 in Hungary if both partners are under 18.

4. On the Verge of Criminalization: Contemporary Harmful Phenomena on the Internet

There are several recently emerged harmful trends in cyberspace that are not covered by the Convention. National legislations however already started to address these issues, which clearly shows a need for criminalization. Letting these issues be tackled on a national level may result in different levels of protection in State Parties which could deepen the chasm between the substantive criminal laws of states. In this section of the article, two issues will be discussed in greater depth, due to the fact that the EU and the Council of Europe have already made attempts to draw attention to these phenomena: the dissemination of sexual content without consent and cyberbullying. While the former is definitely a content-related issue, the latter not necessarily is. The reason this article discusses cyberbullying among content-related crimes is that cyberbullying is an umbrella term that refers to a wide range of online behavior; some of them can be categorized as content-related crimes.

53 Id.

54 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, and replacing Council Framework Decision 2004/68/JHA, Article 2(a).

55 László Dornfeld, 'ICTs and Sexual Exploitation of Children in Europe', *in* Khosrow-Pour Mehdi (ed.), *Encyclopedia of Criminal Activities and the Deep Web*, Hershey, IGI Global, 2020, p. 568.

4.1. Dissemination of Sexual Content without Consent

Non-consensual pornography or "revenge porn" as it is called in layman's terms, has become widespread throughout Europe in the 2010s and the phenomenon is surrounded by scandalous events ever since.[56] A British petition in 2020 called for a ban on the biggest pornography video-sharing platform, Pornhub, because the provider allowed the publication of leaked sex tapes and other types of non-consensual sexual imagery, sometimes featuring minors.[57] Clare McGlynn and Erika Rackley consider the dissemination of sexual content without consent[58] to be imagery that violates personal and bodily integrity,[59] dignity and privacy.[60] Even though the personal harms and detrimental societal impacts of the dissemination of such material are severe, legal response to, and the criminalization of creating and distributing such material is inconsistent with approaches varying from country to country. In the United Kingdom, the Criminal Justice and Courts Act enacted a new offence to criminalize disclosing private sexual photographs and films with the intent to cause distress.[61] The French 'Digital Republic Code' modified Section 226-2-1 of the Penal Code which sanctions the taking or recording or transmitting images of sexual nature of a person in a public or private place without consent (226-1) with two years imprisonment and a fine of EUR 60,000.[62] The German Penal Code does not expressly criminalize the unlawful disclosure of sexual images without consent, however, it sanctions the violation of one's personal life by creating and transmitting images unlawfully.[63] In Hungary, the disclosure of sexual images without consent is not an offence, but the Hungarian Criminal Code protects personal data through several broad provisions. The violation of personal data is

56 In 2018 a popular YouTuber named Chrissy Chambers pursued a civil claim against her British ex-boyfriend who had filmed sexual acts they had engaged in and later published these videos widely on the internet. *See* at www.theguardian.com/technology/2018/jan/17/youtube-star-chrissy-chambers-wins-damages-in-landmark-uk-revenge-porn-case. American politician Katie Hill, who had to resign from Congress in November 2019 because her ex-husband had published explicit images of her, which went viral in the global press. *See* at www.wired.com/story/katie-hill-revenge-porn-facebook. Despite these events, porn sites are still reluctant to remove non-consensual sexual imagery, *see* at www.wired.com/story/porn-sites-still-wont-take-down-non-consensual-deepfakes/.

57 Kate Isaacs, 'Pornhub Needs to Change – Or Shut Down', *The Guardian*, 9 March 2020.

58 Clare McGlynn & Erika Rackley, 'Image-Based Sexual Abuse', *Oxford Journal of Legal Studies*, Vol. 37, Issue 3, 2017, p. 535.

59 Id. p. 545.

60 Id. p. 546.

61 Section 33 of the Criminal Justice and Courts Act 2015: "It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made *(a)* without the consent of an individual who appears in the photograph or film, and *(b)* with the intention of causing that individual distress."

62 Codé Penal 226-2-1: "Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende."

63 Strafgesetzbuch § 201a(1): "Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer 1. von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt eine Bildaufnahme herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt […]."

doi: 10.5553/HYIEL/266627012021009001017

punishable with imprisonment of up to one year.[64] The EU deals with the issue from a privacy perspective. Article 17 of the General Data Protection Regulation (GDPR)[65] ensures that service providers remove personal information upon request, which facilitates the swift removal of sexual content uploaded without consent. However, this privacy-based approach does not offer effective reparation for the victim, nor does it prevent perpetrators from sharing the same images again. Currently, *there aren't any EU legislative instruments to tackle the issue of non-consensual publication of sexual imagery*. The reason for this is that the substantive criminal laws of the Member States are beyond the scope of EU-level harmonization.[66] The Treaty of Lisbon allows for the stronger alignment of national laws in the fields of substantive and procedural criminal laws through the supranational framework of "Judicial Cooperation in Criminal Matters".[67] Still, EU-level harmonization remains limited, "as the Union's competence has been limited to establishing minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crimes with a cross-border dimension."[68] The TFEU lists those offences that are considered particularly serious crimes and as such can be harmonized on an EU level, but the list does not contain content-related offences similar to the non-consensual distribution of sexual imagery.[69] International legal instruments also fail to provide sufficient redress mechanisms. The Istanbul Convention[70] contains several substantive criminal law provisions to criminalize certain forms of violent conduct. It does not mention cyber-related conduct, but any of the behaviors regulated in the discussed sections can be committed in the online sphere. The Cybercrime Convention Committee's (T-CY) mapping study highlights that the Istanbul Convention's explanatory report takes into consideration that threatening behavior may take place in the virtual world (chat rooms, social networking sites, *etc*.).[71] Besides this general remark, the Istanbul Convention does not regulate the dissemination of private images in a separate article and as such, it does not create a straightforward obligation for the State Parties to adopt anti-revenge pornography regulations. The Cybercrime Convention also does not

64 Act C of 2012 on the Criminal Code, Section 219.

65 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).

66 Peter Csonka & Oliver Landwehr, '10 Years after Lisbon. How "Lisbonised" Is the Substantive Criminal Law in the EU?', *Eucrim*, 2019/4, p. 262.

67 Article 82 *et seq*. TFEU.

68 Csonka & Landwehr 2019, p. 262.

69 *See* Article 83 TFEU. These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organized crime.

70 Council of Europe Convention on preventing and combating violence against women and domestic violence.

71 Cybercrime Convention Committee (T-CY), *Mapping Study on Cyberviolence*, Strasbourg, 2018. p. 24.

address cyber-violence and as such it does not mention the dissemination of non-consensual sexual imagery among content-related crimes. Davin Ryan argues that legislation must focus on setting up a preventive framework, which is coherent and repressive of the behavior.[72] Setting up such a framework could be a new path ahead for the further development of the Cybercrime Convention.

4.2. Cyberbullying

Cyberbullying is a term that is used to describe a complex set of issues including harassing, stalking, threatening behavior, the dissemination of libelous, slandering statements. Enacting anti-bullying legislation is one of the regulatory trends of the 21st century. Several countries (such as Canada and the US) introduced anti-bullying legislation which all have a broader scope than cyberbullying as they aim to put an end to all forms of peer violence. In Canada, the province of Ontario was the first to adopt an anti-bullying law (Accepting Schools Act – 2012) to tackle bullying that takes place in schools or in a learning environment.[73] In the US, several states adopted anti-bullying laws in the 2010s. In 2020 New Jersey introduced the Anti-Bullying Rights Acts, in 2011 Connecticut adopted the Act Concerning the Strengthening of School Bullying Laws, and in 2012 California introduced Seth's Law.[74] Regulatory attention has turned toward cyberbullying in Europe in the last couple of years as well. The United Kingdom doesn't have a dedicated legislative instrument to tackle bullying, but anti-bullying measures can be found in several Acts, including the Protection from Harassment Act (1997) and the Malicious Communications Act (1988) and the Communications Act (2003). Germany employs a similar approach, for instead of regulating cyberbullying as a complex issue, German law deals with conducts that are often categorized as bullying separately.[75] Despite its widespread use, it is not a legally defined term since the phenomenon itself lacks a clear definition. The first definitional attempt identified cyberbullying as traditional bullying taking place in the virtual space. The definition used by P. K. Smith *et al*. defines cyberbullying as "an aggressive intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself."[76] A similar definition was coined by Sameer Hinduja and Justin W. Patchin: according to them, cyberbullying is "willful and repeated harm inflicted through the use of

72 David Ryan, 'European Remedial Coherence in the Regulation of Non-Consensual Disclosure of Sexual Images', *Computer Law and Security Review*, Vol. 34, Issue 5, 2018, p. 1072.

73 Shaheen Shariff, *Sexting and Cyberbullying. Defining the Line for Digitally Empowered Kids*, Cambridge University Press, Cambridge, 2015, p. 133.

74 Id. p. 134.

75 The German Criminal Code *(Strafgesetzbuch)* criminalizes the following conducts: incitement to hatred (Section 130), threatening the commission of a felony (Section 241), insult (Section 185), defamation (Section 186), intentional defamation (Section 187), and violation of intimate privacy by taking photographs (Section 201a).

76 Peter K. Smith *et al*., 'Cyberbullying: Its Nature and Impact in Secondary School Pupils', *Journal of Child Psychology and Psychiatry*, Vol. 49, Issue 4, 2008, p. 376.

doi: 10.5553/HYIEL/266627012021009001017

computers, cell phones, and other electronic devices."[77] Further research pointed out that there are significant differences between cyberbullying and traditional bullying due to the anonymity provided by cyberspace, the distance between the perpetrators and victims and the vast dissemination capacities.[78] Shaheen Shariff points out that the word "bullying" is overused[79] by media, academia and NGOs, thus, it is obsolete and unfit to describe the diversity of the issue. Agreeing with this statement the study will use cyberbullying as an umbrella term with the aim of mapping those acts that are often categorized as bullying in cyberspace and identifying those forms of online bullying that are or could be content-related offences. What is common in all the cited pieces of legislation is that they regulate bullying as a behavior that is conducted by children and adolescents in a school environment. Although bullying is indeed behavior that occurs most often among younger persons it is not exclusively committed in an educational setting. Cyberbullying can also be a form of gender-based violence, since research shows that many women experience bullying at their workplace (in the form of sexist jokes, sexist language, gender stereotypes).[80]

Several forms of cyberbullying can be identified in academic literature: online harassment; online stalking; flaming; exclusion; outing (or in other terms doxing); trickery or phishing;[81] identity theft either in the form of impersonation or in its more harmful form, the sockpuppetry;[82] the nonconsensual dissemination of sexual imagery (such as revenge pornography); unsolicited sexting.

The list above is not exhaustive but can be used to illustrate that *some forms of cyberbullying are content-related*. The repeated dissemination of nonconsensual sexual imagery is definitely content related, because it is almost exclusively realized by the dissemination of unlawful content. Harassment and stalking can be considered content-related in specific cases, when the offender targets the victim through public communication platforms (*e.g.* by posting messages to social media timelines or making threatening abusive comments under posts or videos). Harassing behavior in social media is a serious issue; the Pew Research Centre indicates that the majority of online harassment takes place on social media.[83] The Cybercrime Convention does not regulate the above mentioned

77 Sameer Hinduja & Justin W. Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying, Second Edition*, Corwin Press, 2008, p. 5.

78 Anna Costanza Baldry *et al*., 'Cyberbullying and Cybervictimization', *in* Anna Costanza Baldry *et al*. (eds.), *International Perspectives on Cyberbullying Prevalence, Risk Factors and Interventions*, Palgrave McMillan, 2018, p. 4.

79 Shariff 2015, p. 8.

80 Cybercrime Convention Committee (T-CY), *Mapping Study on Cyberviolence*, Strasbourg, 2018, p. 6.

81 Dorothy L. Espelage *et al*., 'Cyberbullying in the United States', *in* Baldry *et al*. (eds.) 2018, p. 65.

82 Sockpuppeting is a relatively new term. A sockpuppet is an account developed with an aim to deceive others. *See* Michael Tsikerdekis & Sherali Zeadally, 'Multiple Account Identity Deception Detection in Social Media Using Nonverbal Behavior', *IEEE Transactions on Information Forensics and Security*, Vol. 9, Issue 8, pp. 1311-1321.

83 Pew Research Centre, *The State of Online Harassment*, at www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/.

content-related conducts under Chapter II, although there are existing examples of regulating the offline form of similar conducts. It must be highlighted that not every behavior considered bullying in nature constitutes a criminal act. In fact, criminal law is on a very far end of the scale and shall only be called upon when all other instruments fail to tackle a certain form of harmful behavior. Distasteful taunts, cruel jokes (even though they are hurtful and cause emotional distress especially to young people whose personalities are not fully evolved) should not be punished by criminal law. Some extreme behaviors such as harassment and stalking are already criminalized by international instruments and national legislation because these are not unique to cyberspace, all of them can be committed through more traditional methods (*e.g.* by speech in front of a large audience, or letters sent *via* postal services). Through these anti-harassment and stalking laws a minimum level of protection is guaranteed, however, owing to their general wording they are unsuitable to reflect the specificities of the virtual forms of these conducts. Therefore, introducing new rules does not seem to be an unnecessary duplication of already existing anti-harassment laws.

5. Procedural Solutions to Tackle Content-Related Offences Online

The Cybercrime Conventions has *a dedicated chapter on procedural provisions in order to aid and enhance the effectiveness of criminal investigations*. Section 2 of the Cybercrime Convention contains procedural provisions which aim to enhance cross border cooperation in evidence gathering while Section 3 deals with the issues concerning jurisdiction which is of paramount importance for the effective investigation of crimes with international elements. Articles 18-21 regulate production orders, the search and seizure of computer-stored data, the collection of traffic data, and the interception of content data (often referred to as wiretapping), respectively. These provisions create an opportunity for the State Parties to oblige private persons and companies such as intermediary service providers to retain and forward data, and to assist law enforcement authorities (LEAs).

5.1. Privacy Issues

As all provisions concern users' personal data and may potentially interfere with the right to private and family life, privacy safeguards are very important. The ECHR protects the right to respect for private and family life in Article 8, whereas private life also includes certain forms of correspondence. The Cybercrime Convention has an article (Article 15) that prescribes the adoption of mechanisms on a domestic level that ensure the adequate protection of human rights, the introduction of judicial or other independent supervision, and the incorporation of the principle of proportionality. A recent survey pointed out that State Parties "are not provided with detailed requirements in terms of protecting fundamental

doi: 10.5553/HYIEL/266627012021009001017

rights and freedoms in the context of data retention."[84] These provisions are too vague as the State Parties were provided with a broad room for maneuver to grant powers to LEAs, without setting limits to the intrusiveness of these powers. It is unclear how the notion of judicial or other independent supervision should be interpreted: should it be connected to the right to an effective remedy, or should it be an authorization preceding the use of such powers? Ryan M.F. Baron draws attention to the fact that the text of the Convention explicitly refers to privacy and "does not specifically state what privacy rights are."[85] The absence of the detailed elaboration of safeguards or competent authorities was a deliberate decision of the drafters of the Cybercrime Convention, as the following reasoning was provided by the explanatory report:

> "the Convention applies to Parties of many different legal systems and cultures [and it is, therefore] not possible to specify in detail the applicable conditions and safeguards for each power and procedure."[86]

Providing effective safeguards with due respect to privacy should be a core consideration, for the right to privacy and LEAs' powers to conduct surveillance or use wiretapping techniques often clash in practice. Several cases found their way to the ECtHR concerning the seizure of computers and data, but also covert investigation techniques such as wiretapping. Thus, there is a pool of judgments that draw attention to the most concerning issues. It has to be noted that the below-mentioned case-law concerns domestic legislation and not the Cybercrime Convention directly. However, such cases demonstrate that State Parties sometimes fail to enact the appropriate safeguards within their respective legal systems, which is a result of

> "the absence of clear guidance on the national transposition of these principles and the identification of 'privacy short-comings' in the actual implementation of the Convention at a national level."[87]

In *Trabajo Rueda*,[88] the ECtHR elaborated on the issue of judicial authorization. The applicant's computer was seized by police in a computer repair shop because the technician noticed that it contained child pornography. The applicant complained that the police obtained the computer without a judicial warrant, thus, the measures interfered with his right to private life and correspondence. The ECtHR examined whether the power to search and seize the applicant's computer was prescribed by law and found that at the time of the commission of the offence, Spain had legal provisions that enabled LEAs to search and seize

84 Data retention in the States Parties to the Budapest Convention on Cybercrime Survey Report 2020 p. 27, at https://rm.coe.int/2088-32-data-retention-report-2020/1680a1f305.

85 Baron 2002, p. 274.

86 Explanatory Report, para. 145.

87 Luca Tosoni, 'Rethinking Privacy in the Council of Europe's Convention on Cybercrime', *Computer Law and Security Review*, Vol. 34, Issue 6, 2018, p. 1208.

88 *Trabajo Rueda v Spain*, No. 32600/12, 30 May 2017.

computers.[89] At the time the Cybercrime Convention wasn't yet ratified by Spain,[90] but it is safe to assume that Spanish legislators were drafting their respective national laws with due consideration to the Cybercrime Convention's procedural provisions. The ECtHR found that *the seizure of the computer violated Article 8 ECHR because it was disproportionate to the legitimate aim (to prevent the sexual abuse of children)*.[91] The ECtHR also highlighted that judicial authorization is a safeguard, which can be circumvented only in case of a matter of urgency: in this case, such urgency had not been identified.

In *Benedik*,[92] the ECtHR evaluated the preservation of dynamic IP addresses and the way police accessed subscriber information. The case concerned the investigation of a peer-to-peer child pornography distribution network (Razorback) which was monitored by Swiss LEAs. The Swiss police retained several dynamic IP addresses; one of them was linked to the applicant by Slovenian police, whose computer was searched and seized after the internet service provider accessed subscriber information and passed it on to the police. The applicant argued that dynamic IP addresses shall be considered traffic data and as such should only be obtainable with a judicial warrant, which was never issued in the case.[93] Besides the relevant domestic law, the ECtHR examined the 1981 Convention and the Cybercrime Convention as well, which defines "traffic data" as

> "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."[94]

The ECtHR emphasized that the rules governing seizure in *Benedik* were foreseeable because the Cybercrime Convention obliges states to introduce measures such as the collection of traffic data and production orders,[95] which the Slovenian Criminal Procedure Act had implemented. However, the ECtHR found that the domestic law that had introduced these measures lacked clarity and "did not offer sufficient safeguards against arbitrary interference"[96] and held that there had been a breach of Article 8 ECHR. *Benedik* well illustrates *what difficulties may arise due to the overly broad rules of the Cybercrime Convention when it comes to safeguards*. Obviously, Article 15 of the Cybercrime Convention laid down the foundations for the protection of certain fundamental rights, yet in the absence

89 Id. para. 38.
90 The applicant was tried and sentenced in 2008, while Spain ratified the Cybercrime Convention two years later in 2010.
91 *Trabajo Rueda*, para. 47.
92 *Benedik v Slovenia*, No. 62357/14, 24 April 2018.
93 Id. para. 15.
94 Id. para. 49.
95 Id. para. 126.
96 Id. para. 132.

of clear instructions or guidance on how to implement these measures, many states failed to design a framework for privacy protection.

5.2. The Role of Intermediary Service Providers in Tackling Content-Related Offences

Intermediary service providers such as internet service providers (ISPs), hosting service providers (such as social media platforms like Facebook and video-sharing platforms like YouTube) play an important role in aiding investigations and mitigating the harms caused by perpetrators. Perpetrators using the internet to disseminate and disclose unlawful content must have internet access often provided by an ISP based on subscription. Many of those offences that are committed *via* the publication or dissemination of unlawful content such as the dissemination of child sexual abuse material, hate speech or incitement to terrorism are frequently committed *via* the services of social networking sites such as Facebook, Instagram or YouTube. Intermediary service providers can support the investigative process and the mitigation of harm by various means. On one hand, they can provide traffic and user data to LEAs, or preserve volatile evidence such as stored data. On the other hand, they have tools to remove or block access to illegal content to stop them from being spread. There are several examples of intermediary providers aiding criminal investigations by providing LEAs with user data. Facebook has received a total of 173,592 government requests for user data in the first half of 2020.[97] In 72.8% of these cases the provider produced some sort of data. The majority of these requests were filed in the US (61,528 requests),[98] but the EU Member States also send requests to Facebook. In the first half of 2020 France and Germany filed 11,086[99] and 11,211 requests, respectively.[100] According to the company, these requests usually seek subscriber information such as name, registration data, IP address logs and account content.[101] Subscriber information is considered personal data and as such, procedural rules and safeguards surround the preservation and transfer of such data.[102] When a criminal investigation is conducted in one country but the requested provider is established in another country, the requested data can be obtained through a mutual legal assistance agreement. Acquiring extraterritorially located data is a time-consuming and long procedure[103] and its revision is underway.

The Cybercrime Convention does not have provisions on the blocking, filtering and removal of illegal content, although taking down or restricting access to unlawful

97 *See* at https://transparency.facebook.com/government-data-requests/jan-jun-2020.
98 *See* at https://transparency.fb.com/data/government-data-requests/country/US.
99 *See* at https://transparency.fb.com/data/government-data-requests/country/FR.
100 *See* at https://transparency.fb.com/data/government-data-requests/country/DE.
101 *See* at https://transparency.facebook.com/government-data-requests/jan-jun-2020.
102 *See* at https://transparency.facebook.com/government-data-requests/jan-jun-2020.
103 Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, para. 123.

content is a common practice in the EU.[104] Namely, the intermediary service providers established in any of the Member States must remove any unlawful content reported, otherwise they can be held liable for user-generated content.[105] A well-known domestic example is the German Act to Improve Enforcement of the Law in Social Networks which obliges intermediary service providers including ISPs and social media service providers to remove content that is unlawful under the German Criminal Code.[106]

6. The Future of the Cybercrime Convention

The current problems relating to the text of the Cybercrime Convention mostly stem from issues of terminology. The Convention *lacks the definition of key terms* such as cybercrime and content-related offences, *leaving a broad margin of appreciation for State Parties* to interpret the provisions of the Convention. It would be welcomed to set common foundations by defining core concepts in order to prevent the divergence of legal systems and to establish a uniform level of protection by obliging State Parties to criminalize the most harmful content-related conducts. Although it would be favorable to expand and change the terminology by amending the Convention in order to maintain the clarity of the text, it is not necessary. The Convention has an Explanatory Report and several guidelines which serve the purpose of clarifying certain provisions.

It can be concluded that *the term child pornography is outdated*. On one hand, the term 'pornography' does not reflect the abuse that is suffered by the victims. On the other hand, pornography can be understood as a term that covers sexually explicit images and materials shared among peers. The Cybercrime Convention's aim is to oblige State Parties to criminalize serious crimes such as conduct related to the sexual exploitation of children and not to stigmatize adolescents who are sharing explicit content. These reasons justify the amendment of the wording of the Convention and the introduction of a term that is better suited to grasp the abusive nature of such conduct, such as child sexual abuse material.

Section 2.3 of this article came to the conclusion that the minimum level approach of the Convention cannot really be criticized as *it is difficult to set forth uniform expectations* when the affected countries differ in terms of legal systems and traditions. However, the threshold could be expanded. As it was mentioned in Section 4, several harmful online behaviors emerged in the last couple of years (such as the non-consensual dissemination of sexual imagery or conducts related to cyberbullying), some of which can be categorized as content-related offences.

104 *See* the Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content prepared by Swiss Institute of Comparative Law, at https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-html.

105 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Articles 12, 13 and 14.

106 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken. § 3. Umgang mit Beschwerden über rechtswidrige Inhalte.

doi: 10.5553/HYIEL/266627012021009001017

In our present days, the list of content-related issues is constantly expanding, and States started to respond to these issues by introducing new laws (*e.g.* the anti-revenge porn laws, and the anti-bullying laws mentioned in Sections 4.1 and 4.2). Thus, the possibility to include some new offences in the Convention would worth considering.

Section 5.1 criticized the Cybercrime Convention due to its broad-brush approach in terms of laying down a framework for the effective protection of human rights. In this section mostly privacy-related issues were discussed. Section 5.2 dealt with the obligations of intermediary service providers, which shall cooperate with LEAs in the signatory states. In this regard, two issues were identified. *(i)* First, extraterritorial data preservation is cumbersome due to the time-consuming mutual legal assistance. *(ii)* Second, the obligations of service providers aim to identify the perpetrator but do not provide for the fate of the illegal content. The swift removal of criminal content is of paramount importance in order to stop the spreading of the content in question.

A partial revision of the text of the Cybercrime Convention is an ongoing process since the drafting of a new additional protocol was announced in 2017.[107] The revisions concern procedural issues that appeared in the last 20 years due to the international nature of cybercrime. Yet they do not concern the terminological issues raised in the previous sections of this study and do not expand the list of substantive provisions. This means that the list of content-related offences will not be expanded in the foreseeable future, leaving the matter of tackling new issues to the domestic legislators. The 2nd Additional Protocol to the Cybercrime Convention will address the issues of language of requests submitted by the LEAs, video conferencing and will hopefully resolve some of the issues that arise in relation to the cross-border collection of electronic evidence.[108] The draft protocol aims to introduce several new measures targeting directly or indirectly service providers that store data that can be used as electronic evidence (such as the IP address, subscriber information, location information, *etc*.).

The *draft of the new Protocol* aims to introduce a new rule about the disclosure of subscriber information.[109] The draft article would enable LEAs to request subscriber information directly from service providers under the jurisdiction of different states. According to the new provisions, such requests may be directly addressed to the service providers instead of requesting assistance from the state in which the provider is established to obtain the necessary information. Parties to the Convention would also be able to request domain name registration information from entities providing domain name services established in another country.[110] The reason behind this provision stems from the fact that the drafters

107 Cybercrime Convention Committee (T-CY), Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime, Strasbourg, 29 November 2017, p. 2.

108 Cybercrime Convention Committee (T-CY), Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Draft Protocol version 3 as approved by the T-CY at its 24th Plenary (28 May 2021).

109 Id. Article 7 – Disclosure of subscriber information.

110 Id. Article 6 – Request for domain name registration information.

recognized: "many forms of cybercrime are facilitated by offenders creating and exploiting domains for malicious and illicit purposes."[111] On the one hand these measures are welcomed because they speed up the investigative process which is of paramount importance when the electronically stored evidence is volatile and is deleted by service providers after a certain amount of time. On the other hand, these provisions raise serious privacy concerns echoed by the European Data Protection Board in a statement issued about the draft protocol. The EDPB pointed out that it is

> "essential that EU negotiating parties ensure that the provisions laid down in the additional protocol do comply with the EU *acquis* in the field of data protection in order to ensure its compatibility with EU primary and secondary law."[112]

The EDPB has expressed its concerns regarding the formerly discussed articles of the additional protocol, especially about the transfer of third party data to non-EU State LEAs. The cross-border transfer of electronic evidence has been on the agenda of the EU legislator as well, since 2018 when the European Commission made a proposal on the text of the e-evidence regulation.[113] The proposed regulation includes the introduction of European Production Orders, which would enable Member States to obtain electronic evidence directly from service providers regardless of their place of establishment within the EU.[114] Such production orders can only be issued by a judge, a court, an investigating judge or by another competent authority;[115] furthermore, the issuing of the orders have must comply with strict conditions.[116] The order shall be necessary and proportionate for the purpose of the proceedings and it shall include information such as the relevant provisions of the criminal law of the requesting state. The European Digital Rights (EDRi) association issued a statement in which it characterized the new regulatory trend of accessing data directly from service providers worrisome[117] and called on the Council of Europe "to create a human rights-respecting alternative to dangerous shortcuts." From this aspect, the additional protocol generates some new problems instead of solving the previously mentioned ones. In a world where crime in the online sphere becomes more and more international in nature, and where national LEAs rely on non-

111 Cybercrime Convention Committee (T-CY), Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime, Strasbourg, 2020, p. 32.

112 European Data Protection Board, *Statement 02/2021 on New Draft Provisions of the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)*, 2021, at https://edpb.europa.eu/sites/edpb/files/files/file1/statement022021onbudapestconvention newprovisions_en.pdf.

113 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.

114 Id. Chapter 2: European Production Order, European Preservation Order and Certificates.

115 Id. Article 4 – Issuing authority.

116 Id. Article 5 – Conditions for issuing a European Production Order.

117 *See* at https://edri.org/our-work/new-protocol-on-cybercrime-a-recipe-for-human-rights-abuse/.

doi: 10.5553/HYIEL/266627012021009001017

state party information more than ever, the Additional Protocol's current text seems to be more of a liability than an asset.