Int J Semiot Law
https://doi.org/10.1007/s11196-024-10179-3

Digital Violence Against Women: Is There a Real Need for Special Criminalization?

Vagia Polyzoidou[1]

Accepted: 2 July 2024
© The Author(s) 2024

Abstract

Social networking and rapid digital evolution have created a brand-new framework of human behaviours and habits. Of course, the majority of them already existed over the centuries but in a different form; as a result, conventional assaults towards legal interests of specific individuals have initially transformed into electronic and then into cyber(-)crimes (p.e. from conventional pornography to internet pornography or cyber/digital pornography including sometimes even virtual pornography via pseudo images and totally AI generated pictures). When discussion comes to gender-based violence, in particular violence against women and domestic violence, we realize that abuses and violations of their fundamental human rights could take place either online or offline; furthermore, both similarities and differences in old and new behaviours, and consequently in crime formations ("actus reus") and in perpetrators' "modus operandi" could easily be found and categorized. This paper will not discover the causes or the elements behind the various digital abuses against women; its first purpose is to gather the various crime behaviours against women and reach some conclusions by a methodically comparative bibliographic and legislative research. Besides, tackling gender-based violence –in particular violence against women and domestic violence- consists one of the main contemporary concerns of every liberal state. CoE's contribution to it –through Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) and Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) but even via ECHR's case law- is indisputable. At the same time, European Union is trying to end gender-based violence through its member states with a new legal instrument (a proposed Directive on combating violence against women and domestic violence), whose results are expected to be more direct and -hopefully- more effective. The main target of this paper is to present and examine the specific form of digital crime against women and girls as long as the majority of crimes nowadays takes place digitally; notwithstanding the fact that pandemic and post pandemic era have definitely determined criminals' modus operandi. At the end of the day, someone has to answer: how Criminal Law faces the new aforementioned behaviours, based on the fundamental theory of legal interest and leading to

Extended author information available on the last page of the article

Published online: 24 July 2024

a justified (extra) standardization? And even more: where does this “plus” in penalties (: aggravation) for behaviours that combine characteristics of digital and gender-based criminality come from?

Keywords Gender-based violence · Digital violence · Cybercrime · Domestic violence · Legal interest · Human dignity · Personal freedom · Personal data · Consent · Intimate image abuse · Obscene images · Fake · Hate speech · Hate crime · Cyber stalking · Cyber harassment · Cyber bullying · Pornography · Criminalization

1 Introduction

Social networking and rapid digital evolution have created a brand-new framework of human behaviours and habits. Of course, the majority of them already existed over the centuries but in a different form; as a result, conventional assaults towards legal interests of specific individuals have initially transformed into electronic and then into cyber(-)crimes (p.e. from conventional pornography to internet pornography or cyber/digital pornography including sometimes even virtual pornography via pseudo images and totally AI generated pictures). When discussion comes to gender-based violence, in particular violence against women and domestic violence, we realize that abuses and violations of their fundamental human rights could take place either online or offline; furthermore, both similarities and differences in old and new behaviours, and consequently in crime formations (“actus reus”) and in perpetrators’ “modus operandi” could easily be found. But how Criminal Law faces the new aforementioned behaviours, based on the fundamental theory of legal interest and leading to a justified (extra) standardization? And even more: where does this “plus” in penalties (: aggravation) for behaviours that combine characteristics of digital and gender-based criminality come from?

2 Approaching the Basic Terms

2.1 Digital Violence

2.1.1 Internet, ICT

The adjective “digital” is connected to any recording or storing information as a series of the numbers 1 and 0, to show that a signal is present or absent -and further to anything using or relating to digital signals and to computer technology; in other words to anything relating to computers and internet.[1]

The pre-existing term in European and international legal bibliography was "computer system" (: an automated, electronic, digitally reprogrammable general-purpose

[1] https://dictionary.cambridge.org/dictionary/english/recording, Assessed 15 May 2024.

system that can process data based on a set of predetermined instructions, the commands collectively called a program). It is a system made mainly of digital electronic circuits and secondarily of electrical and mechanical systems, and its purpose is to process information, while it is also worth noting that every computer system, no matter how big or small, consists of the hardware and the software. Not to mention that nowadays a mobile phone with internet connection is also considered a computer system (therefore not only "smart technology" phones/smart phones). Thus, the use of a computer system that requires the interconnection of computers (through a computer system) in a local network entails essentially the same risks as the internet.[2]

The contemporary term "*Information and Communication Technologies*" (ICT)[3] refers to all technologies that provide access to information through telecommunications. It is, therefore, synonymous with the term "*Information Technology (IT)*" but focuses more on the telecommunications part. It includes the Internet, wireless networks, mobile phones, optical fibers, space systems and of course the various services and applications related to them such as video conferencing services or distance learning, as well as other modern means of communication. It is therefore an "*umbrella*"[4] term that refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, as well as network-based control and monitoring functions.[5] "*Internet*", on the other hand, is defined as the global system of interconnected computer networks, which use an established set of protocols, often called "TCP/IP" (although not all Internet services use this) to serving millions of users every day all over the world. Interconnected computers around the world, which are located in a common communication network, exchange messages (packets) using various protocols (standard communication rules), which are implemented at the hardware and software level.

Lastly, the choice of the phrase ICT aims to ensure that more means are included in the commission of crimes so that it covers in this way the evolution of technology which constantly provides new means and therefore new ways of doing things. Thus, a further expansion of criminal liability is inevitable.

2.1.2 Necessity of Separate Formalization

There is no doubt that the involvement of information systems in the commission of "*traditional*" crimes created a number of new extensions to the various actus reus, mainly standardizing distinct forms (separate standardization and stricter

[2] According to the first article of the Convention on Cybercrime, "electronic system" means "any device or group of interconnected or related devices, one or more of which, according to a program, performs automatic data processing".

[3] http://www.techterms.com/definition/ict. Assessed 15.5.2024.

[4] http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies. Assessed 15.5.2024.

[5] http://www.techopedia.com/definition/24152/information-and-communications-technology-ict. Assessed 15.5.2024.

punishment) of the conventional form. For instance, the form of digital child pornography has been more clearly defined by the phrase "via information and communication technology" in Directive 2011/93/EU, creating a "*non-genuine content related crime*"[6]; which means that the specific form describes the infringement of traditional legal interests (infancy, human dignity, personal data), which is carried out using information and communication technology.[7]

Nevertheless, cyber violence is often referred as a new form of violence, grounded in the increased use of new digital technologies and maximised by the constant connectivity of Web 2.0.[8] In addition to this, it is often considered to be less harmful due to its remote nature. This is an absolute fallacy since it is more of an old problem. Thus, it can start online and continue offline or start offline and continue online[9]; so, it can also come from or lead directly to physical harm. It reflects forms of abuse and victimisation in the physical world that are depicted via digital means, or it may be a precursor to abuse that will be pursued in the physical world.[10] Moreover, according to theory, a perspective grounded in a continuum thinking helps address the harm caused by cyber violence,[11] while this duration of violence[12] and the relation between gender-based violence perpetrated online and offline[13] has been underlined by GREVIO[14] and EU.[15]

The special legislative interest in the separate standardization of digital crimes (otherwise those carried out "via *information and communication technology*") could be explained both empirically and legally. First of all, empirically, the phenomenon of cybercrime has alarmingly large dimensions in the synchronous electronic environment.[16] Furthermore, the standardization as well as the different criminal treatment of digital forms is based on the special technological characteristics of computers and the Internet: easy and fast access to an infinite amount of information in any part of the planet and at any time, without financial cost and effort but with anonymity[17] and privacy for the user-offender, possibility of creating on-line

[6] The non-genuine IT crimes are in turn distinguished into a) behaviours which, although they offend traditional legal goods, their punishment would not be possible without special standardization because they are differentiated from the existing relative legal form of crime and b) criminal acts where the offense arises from the content of the data (content related crimes). See, inter alias, Polyzoidou Vagia [38] p. 298 fn 1005—1009.

[7] So, the crime of online child pornography appears as a "*non-genuine cybercrime*" as it involves the criminalization of conduct that is not exclusively related to cyberspace.

[8] EIGE [8], p. 36.

[9] EIGE, supra n. 6. p. 37.

[10] Van der Wilk A [44].

[11] Kelly L [19] p. 48.

[12] See, inter alias, Esposito E [20] and Esposito E, Breeze R (2022), p. 305 ff.

[13] Lomba N, Navarra C and Fernandes M (2021).

[14] GREVIO, Report [14] Recommendation No 1, https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147. Assessed 15.5.2024.

[15] European Commission Advisory Committee on Equal Opportunities for Women and Men [10] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=1238&NewSearch=1,1. Assessed 15.5.2024.

[16] Grabosky P, Smith R [13] p. 119.

[17] Armstrong H L and Forde P J [3] p 209 ff.

communities between groups (such as pedophiles) which allow the user to obtain a personal environment of expression of his sexual fantasies, direct communication and exchange of material with high digital quality, possibility of sexual pleasure in real time with on-line monitoring, ease of finding pages with relevant content through hyperlinks -links, using different cyberspaces, including social media platforms, messaging applications and discussion sites. The ease of data reproduction, as well as the technical possibilities of their transmission and processing, give many of these acts a different qualitative content. In addition, they pose a greater risk, since minors may be more easily confronted (intentionally or unintentionally) with such material while online.

From a criminological point of view, the minor or less educated/technologically qualified internet user is mainly a vulnerable target ("*website trapping*") appearing as a "*potential*" victim. The perpetrators of these crimes undoubtedly attract more criminological interest; that is why many categories of online criminals are mentioned with various psychological analyzes of their profile.[18] In addition, procedurally, they can easily hide their identity making it difficult for them to be arrested by the police authorities and ultimately making it even more difficult to apply common legal principles in the context of achieving cyber security.

Despite undisputable it is questionable though if the increased indecency of electronic / digital performance should be "*charged*" equally to all behaviours (a classic problem of criminal liability attributed to mere possession/viewing in some cases of crimes, i.e., without any connection to sale /trading). It would probably be preferable for the provision of the special characteristics of information and communications technology to only concern the field of trafficking and the ways of doing it that this includes, as in these cases, mainly, there is undoubtedly the greatest insult to legal interests.

2.2 Gender-Based Violence (GBV)

World Health Organization[19] is pointing out that women and girls face unacceptable rates of violence at the hands of their intimate partners, across the world, while

[18] According to the Australian Institute of Criminology, we can distinguish users into 9 types of perpetrators: (a) herder users, who accidentally come across the material and decide to save it, (b) privately imagined users, who create digital images, through so-called morphing, for private use and satisfaction of their sexual desires, (c) users- "fishermen", i.e. those who look for child pornography on the internet through open gleaning, without communicating with other users, (d) unsafe collectors, who look for material in chat-rooms and on other open levels of the internet, without security (barriers, passwords, etc.), (e) safe collectors, who are members of a closed newsgroup or pedophile group, which maintains secrecy and many security measures, (f) users -groomers, or the so-called groomers, who develop an online relationship with children, to whom they send pornographic material, as a manifestation of their service, (g) natural perpetrators of child abuse in carelessness, who secondarily commit the crime of possession of pornographic material, as manifestation of their pedophilic interests, (h) user-producers, who depict the sexual abuse of children in order to send it to others and (i) user-distributors, who engage in the dissemination of the material and usually fall under some other category of perpetrators cumulatively. See detailed in MFHR (Marangopoulos Foundation for Human Rights), (ed Kioupis Dimitris) [30] p. 20.

[19] World Health Organization [46], https://www.who.int/news-room/fact-sheets/detail/violence-against-women, Assessed 15.5.2024.

pandemic and post pandemic era have definitely increased the phenomenon.[20] Not to mention that the most probable perpetrators are their intimate partners, regardless of their nationality. Additionally, according to EU, gender-based violence (GBV) is an abuse of power and constitutes one of the most serious human rights violations within all societies[21]; UNHCR refers to acts of maltreatment that are directed toward an individual or community because of their gender. It is rooted in gender inequality and reflects harmful norms and practices.[22] GBV as violence that affects persons of a particular gender disproportionately. Today, GBV includes all the forms of violence that are harmful to an individual based on their gender, gender identity or gender expression. Critical feminist considers GBV as a symptom of the unequal power distribution between men and women driven by hierarchical social constructions of masculinity and femininity and perpetrated by men against women in intimate, familial, community and institutional relationships.[23] Besides, the methodological dedication to this specific group of people does not undermine the fact that anyone can experience violence; on the other hand, statistical numbers[24] depict the sad truth that the majority of victims are women and girls. In addition, the abuse that women experience is often repeated, systematic, more severe and more likely to result in injury or death. For this reason, the terms GBV and VAW (: Violence Against Women (VAW) are often used interchangeably.[25]

Institutionally, tackling with gender-based violence -in particular violence against women and domestic violence- consists one of the main contemporary concerns of every politically liberal state. CoE's contribution to it -through Council of Europe Convention on preventing and combating violence against women and domestic violence ('the so-called Istanbul Convention')[26] and Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) but even via ECHR's case law- is indisputable. At the same time, European Union deals with gender issues and the assurance of gender equality in all fields of regulation. In particular, it is trying to end gender-based violence through its member states by becoming the 38th Party to the Convention on Preventing and Combating Violence against Women and Domestic Violence in 2023 and with a new legal instrument, the proposal for a Directive on

[20] See analytically in Speed A, Thomson C, Richardson K [42] p. 540 ff and in Ostadtaghizadeh A, Zarei M, Saniee N, Rasouli MA [37] p. 219.

[21] EIGE, supra n. 6.

[22] https://www.unhcr.org/what-we-do/protect-human-rights/protection/gender-based-violence, Assessed 15.5.2024.

[23] Holt A and Lewis S [15] p. 1–24, Yigang Q, Weilun D, Qunfang W and Zhicong L [48] p. 31.

[24] See analytical figures in Report on Gender Equality in EU [39], Luxembourg: Publications Office of the European Union, 2024, https://op.europa.eu/en/publication-detail/-/publication/44195827-0906-11ef-a251-01aa75ed71a1/language-en, Assessed 15.5.2024.

[25] According to Rogers and Ali "*it is important to note, however, that GBV intersects the boundaries of gender, age, ability, socioeconomic class and sexual identity as well as those denoted by culture, religion and ethnicity. As such, an intersectional lens should be used to understand GBV in any context*", Rogers M, Ali P [40] p. 4.

[26] According to Court of Justice of the European Union in its judgment of 16 January 2024 "*areas of EU law which fall within the exclusive competence must be interpreted consistently with the Istanbul Convention, even by Member States that have not yet ratified that Convention*".

combating violence against women and domestic violence[27] of the European Parliament and of the Council on combating violence against women and domestic violence whose results are expected to be more direct and -hopefully- more effective.[28]

2.3 A combination: Cyber Violence Against Women -and Girls (CVAWG)

Digital technologies have simplified well-known abusive behaviours by providing convenient tools for abusers to access their targets; they are simultaneously opening the door to new forms of abuse that require technology, such as the non-consensual creation of sexual images of women through artificial intelligence.[29] So, how is cyber violence "*gendered*"? Both women and men may experience incidents of interpersonal violence and abuse (including online): men can be victims too, and women can be perpetrators. However, evidence at EU, international and national levels show that women and girls are highly exposed to cyber violence and are particularly affected by this phenomenon[30] and more likely to experience repeated and severe forms of physical, psychological or emotional abuse and to suffer from severe consequences.[31]

CVAWG includes a range of different forms of violence perpetrated by ICT means on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or personal beliefs). In fact, there is a great variety of criminal behaviours that contain digital violence vs women (analytically below) and even more forms of cyber violence (e.g. impersonation and identity theft, doxing, flaming, trolling and body shaming) that are still not taken into consideration as they were not frequently defined in the majority of Member States, or were deemed "*as either too generic (e.g. online threats), too specific (e.g. impersonation) or falling under the general provisions on other forms of violence, like cyber harassment*".[32] Cyber violence against women and girls (CVAWG) is indisputably both a new and the greater new dimension of gender-based violence.

[27] The Directive criminalises physical violence, as well as psychological, economic and sexual violence against women across the EU, both offline and online. It is characterized as "*a milestone—the first comprehensive legal instrument at EU level to tackle violence against women, which is still too pervasive in the European Union. With this directive all victims of violence against women and domestic violence across the European Union will benefit from the same comprehensive set of measures of protection, support and access to justice*.".

[28] All the aforementioned are complimentary to the proposal for a Regulation on preventing and combating child sexual abuse online adopted in May 2022 as long as to a proposal to update the criminal law rules on child sexual abuse and sexual exploitation. See, also, the Anti-Trafficking Directive.

[29] Dunn S [6], p. 51 ff, de Silva R [5].

[30] EIGE, supra n. 6 and [12], https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf, Assessed 15.5.2024.

[31] GREVIO, supra n. 12 [14].

[32] EIGE, supra n. 6, p. 2 ff.

At UN level,[33] the Special Rapporteur on VAW clearly defined gender-based cyber violence as: any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.[34] Council of Europe (CoE), in its monitoring of the implementation of the legally binding Istanbul Convention[35] -and specifically the CoE Expert group on action against violence against women and domestic violence[36]- identified that national-level laws and policies often overlook the digital dimension of VAWG, underlying "*that there is no universal typology/definition of behav- iours or action that is considered to group together all forms of violence against women perpetrated online or through technology*".[37]

In EU level, there is no harmonised legal definition of CVAWG except for the following that emerges from a non-containing criminal provisions (and consequently a non binding) text, according to which: *"Cyberviolence against women is an act of gender-based violence perpetrated directly or indirectly through information and communication technologies that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering to women and girls, including threats of such acts, whether occurring in public or private life, or hin- drances to the use of their fundamental rights and freedoms. Cyber-violence against women is not limited to but includes violations of privacy, stalking, harassment, gender-based hate speech, personal content sharing with- out consent, image-based sexual abuse, hacking, identity theft, and direct violence. Cyberviolence is part of the continuum of vio- lence against women: it does not exist in a vacuum; rather, it both stems from and sus- tains multiple forms of offline violence".*[38]

[33] UN Human Rights Council, 2018.

[34] Beyond this policy definition, the UN has addressed the issue of CVAWG through various resolutions (e.g. the UN General Assembly resolution on protecting women human rights defenders and Human Rights Council resolution 34/7) and multiple recommendations of the Committee for the Con- vention on the Elimination of All Forms of Discrimination against Women (CEDAW). In addition, both the fifth sustainable development goal (SDG 5) and the Beijing Platform for Action for Equality, Development and Peace (BPfA) aim to eliminate all forms of violence against women and girls.

[35] Both Istanbul Convention (Article 3a with its definition of '*violence against women'* that includes all acts of gender-based violence, Article 33 on psychological violence, Article 34 on stalking and Article 40 on sexual harassment) and Budapest Convention on cybercrime and additional protocol (Articles 4 and 5 relating to data and system interference which may cause death or physical and psychological injury) as well as Lanzarote Convention on protection of children against sexual exploitation and sexual abuse (Articles 18 to 23) can be applied to CVAWG. Even the existing international human rights framework can address CVAWG in the context of ECHR (See Article 3—prohibition of torture, inhuman or degrading treatment or punishment; Article 8—right to respect for private and family life; Article 10—freedom of expression; Article 13—right to an effective remedy; and Article 14—prohibition of discrimination).

[36] O' Rourke Scott L [35].

[37] GREVIO, supra n. 12.

[38] European Commission, supra n. 13.

3 The Crimes' Categorization

3.1 The Criterion: Legal Interest

Given the aforementioned conclusions, general necessity of punishing behaviours that meet the criteria of CVAWG is almost clear. Nevertheless, the answer to the crucial question of necessity (or not) to criminalize a behaviour should be based on the existence of a specific legal interest that has to be protected by the specific behaviour.[39] The special need to address these phenomena on a common basis stems from the serious impacts of them on the core EU values enshrined in Article 2 of the TEU. There is no doubt, after all, that EU framework supports such criminalization via Article 83(1) of the TFEU[40] as long as targeted persons are selected based on their real or perceived connection, attachment, affiliation with, support or membership of a community or a group sharing a protected characteristic while the perpetrator's motive is key in distinguishing these offences from other crimes and in determining their greater gravity having regard to the specific impact that these offences have on the individual victim, on communities and on society at large. Lastly, the umbrella of CVAWG includes crimes (some of them versus human dignity) that belong to an area of particularly serious crime as long as they oppose to tolerance and equal dignity of all human beings that constitute the foundations of a democratic, pluralistic society.[41]

So, which is the specific legal interest that is harmed or at stake by committing crimes that are included to CVAWG term? The theory of legal interests could help as by grouping the relevant actions. The crimes that fall under the CVAWG "umbrella" could be categorized in the following categories:

[39] According to Manoledakis, legal goods are (material) objects of the external world, perceived with our senses, or physical or social properties of these objects, which satisfy vital needs—and serve the corresponding interests—of the members of society, thus constituting essential elements of social life. The objects that constitute legal goods have at every moment a physical or social destination within the space, satisfying some need (that is, they have meaning). This vital importance creates an interest either in the person who owns or embodies the object or property or in the social group (when the need that is satisfied belongs to it) in the preservation of the good. See, inter alias, Manoledakis I [27] p. 151–155, Manoledakis I [28] p 88–156.

[40] Besides Article 83(1) of the TFEU allows the Council to identify additional areas of crime provided they fulfil specific criteria if the new area must be of particularly serious crime, with a cross-border dimension resulting from the nature or impact of the offences or from a special need to combat them on a common basis.

[41] The ECtHR considered that it may be necessary in "*democratic societies to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance while it further pointed out that criminal sanctions against individuals responsible for the most serious expressions of hatred, inciting others to violence, could also be invoked as a last resort measure*". For these reasons, the ECtHR consistently recognised in case-law that the right to freedom of expression does not prevent criminal law responses to certain forms of hate speech.

3.2 Crimes Versus Human Dignity

3.2.1 Non-consensual Intimate Image Abuse

As long as pornography is usually related to adult pornography, contemporary academic literature seems to substitute the terms of child pornography[42] with child sexual abuse material and revenge porn or even non-consensual pornography with non-consensual intimate images; that's why non—consensual intimate image abuses is considered more appropriate to be used as an "*umbrella*" term. First of all, the criminalization of consensual indecent images that come from adults[43] could be justified on a legal interest beyond sexual order or morals[44] –but focused on the sexual self-determination of minors and the protection of youth/infancy. On the other hand, child sexual abuse material or the so-called child pornography is not just a kind of pornography but an extremely complicated crime in terms of substantive criminal law. Not only because of the various forms of the crime but also because of the different legal interests that are hidden behind every aspect[45] and a highly protective rationale behind its criminalization that leads sometimes to punishment even if there is not direct harm to children -or even in abstracto. Not to mention than consensus (: consent) could not be conceived in this place since minors could not provide a valid consent, lacking the right of sexual self-determination.

Non-consensual intimate image abuse refer to any type of audio-visual archive (images/videos) that could be obtained non-consensually, manipulated non-consensually, or obtained consensually but distributed non-consensually; furthermore non-consensual intimate image abuse involves the distribution through ICT means or the threat of distribution through ICT means of intimate or private images/videos without the consent of the subject (usually of a woman or girl). Most frequently recurring types of conduct are the dissemination, the publishing online non-authorised intimate archives, the online grooming or even voyeurism/creepshots. Common motivations include sexualising the victim, inflicting harm on the victim or negatively affecting the life of the victim. The acts can: a. start online and continue offline; b. start offline and continue online; c. be perpetrated by an unknown person

[42] Nonetheless, the term "*child pornography*" has been recognized as inappropriate while "abuse images" is considered as a suitable one. See Quayle Ethel [17] p. 26, Leary MG [21] p. 1 ff.

[43] See in detail Feinberg Joel [11] p. 567 ff.

[44] ECtHR has already suggested the replacement of "*morals*" and "*prudency*" in national legal instruments for indecent images from terms such as "*protection of the youth and childhood purity*".

[45] EU dealt with the criminalization of child pornography –after several amendments of the initial proposal- in Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA. According to article 5 of Directive 2011/93/EU "1. Member States shall the necessary measures to ensure that the intentional conduct, when committed without right, referred to in paragraphs 2 to 6 is punishable". However, art. 5 par. 7 and art. 8 provide the member states with the discretion of non-criminalizing certain behaviours of child pornography. The criteria that are used for the exclusions of the criminalization are indicative not only of the protected legal interests but also (sometimes) of harm's absence (or its "negligible presence"). [Nevertheless, we could not ignore that there is only discretion –while the criminalization of the relevant behaviours is obligatory.].

to the victim; d. be perpetrated by someone who is/was in an (intimate) relationship with the victim. Besides, it is crystal clear that the (non) consent is the basis of standardization.

Consent is one of the most crucial notions in the field of criminal law; it is also very important in the field of legal methodology[46] at many different levels.[47] Besides, feminist theory has contributed not only to realizing the importance of consent but also to the understanding of its complexity.[48] The non-consensual sharing of intimate and sexual images covers a wide variety of abusive digital practices. Sexual images can be circulated on secret online fora, shared in private messages, uploaded to commercial porn sites and social media, or even used to create fake dating and escort profiles. The pictures and videos can be produced with consent or coercion; they can be taken without the victim's knowledge, they can be edited to show a sexual situation that never actually happened, or they can even document a physical sexual assault. Regardless of the origin and distribution history of an assaulting image, sharing of the image constitutes a type of gendered sexual violence that has specific mediated impacts on victims' lives and consequently requires specific coping methods and interventions.[49]

3.2.1.1 Criminalizing Fake/Virtual Intimate Images There is a great discussion on criminalizing the behaviours (from production to mere possession) that relate to non—real images as well as to the criteria that should be used.[50] For the reasons of this paper, it is necessary to distinguish the following categories[51]:

1) Nonrealistic pictures, e.g., cartoons, anime, manga, hentai etc.
2) Realistic pictures, which came from modification of a picture depicted at least one real person –that is the so-called procedure of "morphing" (through photoshop, photopaint, apecture, adobe premiere, adobe aftereffects etc.). For instance: deep fakes.

[46] "Consensus" is the touchstone in discussion for paternalism and self-determination. See Dworkin Gerald [7].

[47] See Asp P, Ulväng M [1] 417 ff.

[48] For Feminism and Queer Theory see inter alias Bibbings L, Nicolson D, [4].

[49] Uldbjerg S [43] p. 529.

[50] For instance, Powell et al. (2019) suggest a categorization framework that groups image-based sexual abuse into five subcategories: relationship retribution, sextortion, voyeurism, sexploitation and sexual assault, focusing on the acts of the aggressors. On the other hand, Uldbjerg suggests as criterion the (lack of) consent and specifically: "*the first category, consensually produced sexual images, covers cases where the assaulting act was the image distribution, while the production of the image and the sexual situation were consensual; the second category, non-consensually produced images, covers cases where the distribution and production of the image were non- consensual, but there was, apart from the image production itself, no immediate non-consensual sexualization happening; the third category, repurposed images, covers cases where the image was produced with consent, but later edited or reused in sexualizing contexts, making the sexualization and distribution non-consensual; the fourth category, coerced images, covers cases where the distribution, produc- tion and sexualization were non-consensual, meaning that image production and distribution are part of, but do not solely constitute, a case of sexual violence*". See, Uldbjerg S, ibid, p. 530.

[51] See Polyzoidou, supra n. 14. p.179.

3) Computer generated imagery[52] (digitally manufactured realistic pictures[53]). For instance: ideograms.

The ratio in criminalizing acts of material which belongs to the second category is obvious[54]: the protection of depicted person' s human dignity as he/she seems to participate in sexual activities as a protagonist. Not to mention that even AI Act[55] deals with deep fakes in general, while the VAW-DV Directive explicitly criminalises the non-consensual sharing of material that make it appear someone is engaged in sexually explicit activities. The VAW- DV Directive also foresees prompt removal and disabling access to illegal material tackling further "*algorithmic bias*" (including gender bias) and propose transparent approaches and best practices at various stages of the algorithm development process, in the training of datasets and in AI-generated decision-making.

However, criminalizing the other forms of virtual material is neither obvious nor indisputable[56] -since there is not a real protagonist whose interests are in jeopardy.[57] As a result, searching deeply for "*harm*" (in two fundamental dimensions[58] emerging from relevant discussion in the field of (de)criminalization of child pornography[59]) is a "conditio sine qua non"; otherwise, the foundations of criminalization will be weak.

[52] http://www.sciencedaily.com/articles/c/computer-generated_imagery.htm, Assessed 15.5.2024.

[53] It is worth mentioning that the first simulation of electronically modified images with photographs depicting real minors is found in Fellows and Arnold/The Birmingham University Case in: *R v Fellows*, *R v Arnold*, as well as in Akdeniz Y [2] p 223 ff, Yar M [47] p. 118 ff.

[54] Ost S [36], p. 127–131.

[55] The AI Act explicitly requires labelling of deep fakes, meaning AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful. For instance, the deployer of an AI system that generates a deepfake, is to disclose that the content has been artificially generated or manipulated. The provider of generative AI systems must employ technical solutions that enable the marking and detection of that the content has been generated by AI. There are also specific obligations for providers of most impactful general purpose AI models presenting systemic risks to take measures to assess and mitigate risks of the generation and dissemination of harmful, illegal and discriminatory content.

[56] On the contrary, criminalizing the "pseudo-pornography (even of minors)" (the possession of pseudo-images in particular) was strongly condemned because of the absence of a real depicted child, Nair A [32] p 226, Morgan L [31] p. 31ff.

[57] It has been argued that the only rationale of criminalizing virtual child pornography is the creation of eroticism among non-equals which harms primarily the women (even when it comes to child pornography). See Levy N [22] p. 322.

[58] See Quayle, supra n. p. 9.

[59] See Polyzoidou, supra n. 14., demonstrating the different level of harm (and consequently the different way or measure of infringing the legal interest affected), unlike what could be assumed by the initial collective provision of all forms of virtual pornography in the definition of child pornography from the 2011/93/EU. In addition, the mentioned exclusions contribute to avoiding an infringement of principle of legality and an unconstitutional punishment of (free) thinking.

3.2.2 Online, gender-Based, Hate Speech and Hate Crime

Hate crime[60] is a crime committed against one or more persons whose victimization is chosen precisely because of their specific characteristics, which constitute their unchanging identity by making them members of a specific group. As a rule, the foundational characteristics of the particular category of crimes, and those which in practice were first introduced into the law, are race, national origin and nationality, while religion follows. Other fundamental characteristics in the individual national legislations are gender, age, mental or physical disability, and sexual orientation while rarely occurring characteristics such as ideology, relationship with politicians' organizations, gender identity, marital status, social status, etc.[61]

In general, hate crime include any behaviour that depicts opposition to any form of someone's particularity, from opposition to a different race and other biological characteristics to the different manifestations of a person's cultural and sexual identity; in other words as the ideology or practice aimed at selectively discriminating against a group of people, members of society, on the basis of a set of common characteristics, which the members of the group bear and which, objectively, do not affect the ability of the members of the group to participate in the fundamental functions of society.[62] Besides, the recipients of racist behaviour are mainly immigrants, but also Roma, Jews, Muslims, transsexuals and LGBTI people in general, etc.; unfortunately, in the majority of the relevant cases, the victims of racist attacks do not resort to the police or justice due to fear of deportation, revenge attacks, etc.[63]

More specifically, online gender-based hate speech is defined as content posted and shared through ICT means targeting mainly women and/or girls because of their gender, or because of a combination of gender and other factors (e.g., race, age, disability, sexuality, ethnicity, nationality, religion or profession).[64] It can also involve posting and sharing, through ICT means, violent content that consists of portraying women and girls as sexual objects or targets of violence. This content can be sent privately or publicly and is often targeted at women in public-facing roles.[65]

Lastly, according to EIGE,[66] most frequently recurring types of conduct are inciting discrimination, hostility or violence, condoning, denying or trivialising international crimes while the distinguishing criterion between gender-based online hate speech and other forms of violence is mainly the use of ICT to send demeaning, unwanted, cruel remarks, citing the victim's gender and spreading hateful language targeted at women and girls.

[60] The term "*racist crime*" seems lastly to be rejected and be substituted by the term "*hate crime*" -as racism presupposes the admission of different races existence.

[61] Lima D [23], pp. 15—18.

[62] See also Schmid W T [24] pp. 31–40.

[63] Neller J [33] pp 39 ff.

[64] EIGE, supra n. 6, p. 50.

[65] Kavanagh E, Brown L [18] p. 1380 ff.

[66] EIGE, supra n. 6., p. 52.

3.2.3 The Legal Interest of Human Dignity

The legal interest that is primarily affected by hate speech but even by non-consensual images abuse is human dignity as it is harmed in any case where the victim is considered by the perpetrator to be "*inferior*" to the rest of the people.

Today, human dignity could be considered as a legal interest in criminal law (not only as fundamental constitutional principle). In particular, in Germany for the first time an attempt was made to differentiate the absolutely inviolable core of human dignity (which must enjoy absolute protection) from its periphery. Undoubtedly, the basic concept of human dignity is primarily a constitutional principle and a philosophical basis with very important consequences in general. However, human dignity can also be recognized as a legal interest whenever the capacity for human self-determination is negated to the point where human existence is annihilated. In other words, when a person is used as an object and not as a subject (as typically happens in cases of state action using torture or in cases of slavery of a person), her human dignity is violated—and only with this conceptual content can human dignity be understood as a legal good. So, criminally speaking, human dignity has a much more specific content (in comparison to constitutional law); as a result, we can find an offense towards human dignity when X uses Y as an object (see "Instrumentalisierung[67]": objectification) and that' s exactly what happens when X uses pornographic material depicting Y for his sexual satisfaction, for example.

At the same time, the notion of human dignity should not be confused with the legal interest of honor or reputation. The first is related to the existence of any human as a self-defined being that is not allowed to be treated as an object, while the second is a social attribute to any human individualized in his (social) appearance. The legal interest of honor does it have its own semantic content; furthermore, honor is secondarily offended in each of the crimes this paper deals with (and in the majority of crimes against personal legal interests, except for crimes against property/financial crimes).

3.3 Crimes Versus Personal Freedom

3.3.1 Cyber Stalking

Cyber stalking against women and girls involves intentional repeated acts against women and/ or girls because of their gender, or because of a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or beliefs). It is committed through the use of ICT means, to harass, intimidate, persecute, spy or establish unwanted communication or contact, engaging in harmful behaviours that make the victim feel threatened, distressed or unsafe in any way. Most frequently recurring types of conduct are: threatening, intimidating, harassing, establishing unwanted communication, monitoring, spying, pursuing, following, sharing intimate

[67] For the term "Instrumentalisierung des Kindes" in Hörnle T [16] p. 427.

photos without consent with obsessive intent, sending/posting offensive messages, insults, slander, denigration.

3.3.2 Cyber Harassment

Cyber harassment against women and girls involves one or more acts against victims because of their gender, or because of a combination of gender and other factors (e.g. race, age, dis- ability, profession, personal beliefs or sexual orientation). It is committed by one or more people in a "network"[68] through the use of ICT means to harass, impose or intercept communication, with the purpose or effect of creating an intimidating, hostile, degrading, humiliating or offensive environment for the victim. Most frequently recurring types of conduct are harassing, tracking, pursuing, intercepting, abusing personal data, sending/posting offensive messages, sexual comments, defamation.[69] In addition to this, sending abusive text messages, sending unwanted gifts, making frequent, unwanted communications, such as telephone calls, text messages or other online contact, for example via social networking sites, making hang-up telephone calls, stealing or reading mail are considered as cyber harassment in literature.

Notwithstanding the importance of its criminalization, cyber harassment seems less severe to cyber stalking in terms of frequency, aggressiveness, obsess of perpetrators since the last one (: cyber stalking) contains repetition of stalker's behaviour and the creation of continuous threat or unsafety to the victim in any way.

3.3.3 Cyber Bullying

Cyber bullying is defined as sending or publishing offensive/malicious material or engaging in other forms of social aggression via the Internet or other digital technologies. In traditional bullying, we observe "*the deliberate and conscious desire to harm another and put him/her in a situation of pressure*". Therefore, the victim simply happens to be there, "*repeatedly exposed, when negative acts occur*," as Olweus aptly observes.[70] The difference between traditional bullying and cyberbullying is that its effects have a greater impact because the Internet is accessed by a particularly large number of people, so it is more public than traditional bullying. Nevertheless, the reasons for the manifestation of this behaviour are focused on the educational context (disagreements between students, playful mood, strictness and negative grading of teachers, parents' dissatisfaction with their children's friends and anonymous expression of threats). So, cyberbullying generally comprises

[68] Harassment can be done by a single person, such as an ex-partner or an online stalker; however,the internet has provided spaces for people to organize and encourage larger-scale coordinated attacks by groups of abusers. Marwick and Caplan (2018) describe this type of abuse as "networked harassment". See in detail in Dunn, supra n. 30. p. 8.

[69] In many countries, the legal definition of defamation includes publishing false information about someone that harms their reputation, for example by publishing false information about somebody online, so as to be found by a mere Google research.

[70] Olweus D [34], pp. 53ff, 71–72, 82, 101—103.

sending threatening or otherwise nasty messages or other communications to people via social media, gaming sites, text or email, posting embarrassing or humiliating video on hosting sites such as YouTube or Vimeo, or harassing through repeated texts, instant messages or chats,[71] trolling, sending threatening, disturbing messages, ridiculing, teasing, offending, insulting, impersonating.[72]

Although cyber bullying is -in general terms[73]- considered significantly more harmless to the aforementioned "*cyber-behaviours*", its effects range from annoyance and mild distress to—in the most extreme cases—self-harm and suicide. This can be a reality for vulnerable people, or indeed anybody made to feel vulnerable through cyberbullying or other personal circumstances.

3.3.4 The Legal Interest of Personal Freedom

3.3.4.1 Personal Freedom as Generic Legal Interest The legal interest that is primarily affected by behaviours like cyber stalking/harassment/bulling -that deprive the victim of the right to self-determination as well as from the feeling of security- is personal freedom.

Personal freedom is one of the fundamental human rights, the most important after the right to life, since the rest of the individual rights, public and private, are derived from it, and their exercise also depends on it. The right to freedom is inalienable and each individual cannot waive it, i.e., he cannot be deprived of his freedom or remain without it. It was established in the Constitutions of all liberal and democratic societies -contrary to totalitarian ones- as one of the most important human rights directly intertwined with the Rule of Law. Personal freedom is a natural property of the human being. In liberal and democratic systems, personal freedom is a supreme social value and a necessary condition (sine qua non) for the existence and maintenance of the structure of society. Therefore, due to the important social role it performs, it has been reduced to a size worthy of criminal protection, i.e., a legal interest.

In theory, many views have been expressed regarding the definition of personal freedom. A common characteristic of most of them is that, on the one hand, they describe personal freedom as a multidimensional legal interest with more than one aspect and, on the other hand, that they reduce all its individual aspects to freedom of will and the freedom to exercise it. Any expression made without the individual's own will, i.e., with external intervention, cannot be characterized as free, by default. As its first characteristic is concerned, it is crucial to say that the right to privacy (see also personal data) and self-determination consists one of personal freedom's fundamental aspects.

[71] https://www.getsafeonline.org/personal/articles/online-abuse/, Assessed 15.5.2024.

[72] EIGE, supra n. 6, p. 47.

[73] There is a kind of controversy since Olweus characterizes cyberbullying as "*abuse*"; whereas Smith, prefers the term "conflict". See Smith P K, Cowie H, Olafsson R F, & Liefooghe A P [41] p. 1120 ff.

3.3.4.2 Privacy—Personal Data The concept of personal data is perceived as part of somebody's personal freedom to maintain a strictly private information space, to which only he/she can allow access (informatics self-determination). Besides, the protection of citizens' private life (the content of which includes, among other things, personal data) is constitutionally guaranteed—as a (relatively) inviolable individual right, while the criminal protection of privacy has also increased in recent years.

As "personal data" is defined any information that refers to a natural person, whose identity is known and can be ascertained, i.e., an identified—identifiable person while as "*sensitive data*" (with increased protection) are considered, among other things, the sexual life of persons. The disclosure of information, which falls under the category of sensitive personal data, entails increased risks for the individual, affects the sphere of the privacy of his private life and thus more strongly infringes on his privacy, i.e., the privacy of his private life. The protection of personal data seems to have been a particularly popular subject (and) of scientific interest in recent years—and indeed by authors of various legal branches, as the provisions of the relevant law concern both administrative and civil and of course also in the criminal field. The result of this is the adoption of various definitions, the content of which several times overlaps, and the corresponding design of legal interest (privacy, private life in the form of informational self-determination, self-determination of personal information), which are often confused with constitutionally guaranteed individual rights (the right to informational self-determination) and with primary values for a rule of law. Criticism, however, of the above opinions does not fall within the framework of the development of this specific work.

Information related to the person's love—sexual life—are highly personal and for this reason constitute by law sensitive personal data, while furthermore their disclosure by a third party seriously infringes the private life of the person. Even if someone's sexual life does not present particularities, the disclosure of its individual aspects implies an invasion of his private life, as in the context of their social interaction, individuals do not reveal these details. Thus, the publication of private sexual material during acts or events of their love life -in other words any public disclosure of private information- is a violation of privacy (whether the subject of the material is a minor or an adult). The aforementioned practices are common in the circle of gender-based violence by perpetrators in order to harass, embarrass and harm the reputation of their targets (*R. v. Fox*). In fact, the violation of personal data should be understood as damage to the privacy of each individual—regardless of whether this damage also endangers other traditional individual legal interests of citizens.

4 Conclusion

The identification of the legal interests protected simultaneously with the highlighting of the particular similarities of specific criminal behaviours -and its relevant categorization—can help not only to a clearer delimitation of criminal offenses but also to an adequate justification of the very need for a diversified criminalization. As emphasised by GREVIO, ignoring the gender pattern associated with cyber violence risks missing the social reality of CVAWG stemming from stereotyped gender roles

and the presupposed inferiority of specific group of people (women and girls) versus another. In fact, gender is a strong predictor of exposure to abuse on digital media while the coexistence with other vulnerable characteristics (e.g. race and ethnicity, body characteristics -especially wage and fat-, sexual orientation, disability or profession) could multiply the chances of being victimized.

Today, at national level, most EU Member States recognise some form of cyber violence following one of the following schemes[74]: 1. cyber violence is covered by general offences with no reference of any kind to ICT or other means; 2. cyber violence is covered by general offences but with reference to ICT or other means; 3. cyber violence is considered an aggravating circumstance of general offences; 4. cyber violence is covered by specific legal pro- visions. However, only a few Member States have legal provisions specific to cyber violence and, when these exist, they tend to be gender neutral, with no reference to CVAWG -or even to GBV.

As long as criminalization consists the ultimum ratio and ultimum refugium in the fight of crimes, every suggestion for criminalization or increasing of penalty should be based on a "*plus*" in criminal behaviour that stems from an "*added demerit*" of the action or of the perpetrator. A common approach to the criminalisation of every aspect of CVAWG (for example introducing aggravating factor of general offense) can ensure a consistent protection of the victims of such acts across the EU.[75]

Funding Open access funding provided by the Cyprus Libraries Consortium (CLC).

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Asp, P., and M. Ulväng. 2017. Consent in Sweden. In *Domestic and Comparative Perspectives, Substantive Issues in Criminal Law*, ed. A. Reed, M. Bohlander, N. Wake, and E. Smith, 417–434. Rootledge.

[74] See EIGE, supra n. 6.

[75] See also Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA. Given the cross-border dimension of hate speech and hate crime, and the need for a criminal law solution, cooperation between judicial authorities will be crucial. A common criminal justice response can improve mutual trust and judicial cooperation which are the basic principles of an EU area of freedom, security and justice with respect for fundamental rights.

2. Akdeniz, Y. 1997. Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach. In *Law and the Internet: Regulating Cyberspace*, ed. L. Edwards and C. Waelde, 223–241. Hart Publishing.
3. Armstrong, H.L., and P.J. Forde. 2003. Internet Anonymity Practices in Computer Crime. *Information Management and Computer Security* 2003: 209–215.
4. Bibbings, L., and D. Nicolson. 2000. *Feminist Perspectives on Criminal Law*. Cavendish Publishing.
5. de Silva, R. 2023. A Rapidly Shifting Landscape: Why Digitized Violence is the Newest Category of Gender-Based Violence (November 29, 2023), SciencesPo Law Review, forthcoming, U of Penn Law School, Public Law Research Paper No. 23–43, Available at SSRN: https://ssrn.com/abstract=4648409, Assessed 15.5.2024
6. Dunn, S. 2020. Technology-Facilitated Gender-Based Violence: An Overview. Centre for InternationalGovernance Innovation: Supporting a Safer Internet Paper No 1, online: https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/, Assessed 15.5.2024
7. Dworkin, G. 2017. Paternalism. In: Zalta E. (ed.), The Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/archives/win2017/entries/paternalism/, Assessed 15.5.2024
8. EIGE, Gender-based violence. Combating Cyber Violence against Women and Girls, Luxembourg: Publications Office of the European Union, 2022
9. Esposito, E., and R. Breeze. 2022. Gender and Politics in a Digitalised World: Investigating Online Hostility Against UK Female MPs'. *Discourse and Society* 33 (3): 303–323.
10. European Commission Advisory Committee on Equal Opportunities for Women and Men. 2020. https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=1238&NewSearch=1,1. Assessed 15.5.2024.
11. Feinberg, J. 1979. Pornography and the Criminal Law. *University of Pittsburgh Law Review* 40: 567–604.
12. FRA. 2014. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf , Assessed 15.5.2024
13. Grabosky, P., and R. Smith. 1998. *Crime in the Digital Age*. Transaction Publishers.
14. GREVIO Report. 2021. Recommendation No 1, https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147. Assessed 15.5.2024
15. Holt, A., and S. Lewis. 2024. (2024) A Sense of Danger: Gender-Based Violence and the Quest for a Sensory Criminology. *Feminist Criminology* 19 (1): 3–24.
16. Hörnle, T. 2005. *Grob anstößiges Verhalten, Vittorio Klostermann*. Frankfurt a. M.
17. Quayle, E. 2004. The Impact of Viewing on Offending Behavior. In *Child Sexual Abuse and the Internet: Tackling the new frontier, Martin C*, ed. M.C. Calder, 1–30. Calder: Russell House Publishing, Dorset.
18. Kavanagh, E., and L. Brown. 2020. Towards a Research Agenda for Examining Online Gender-Based Violence Against Women Academics. *Journal of Further and Higher Education* 44 (10): 1379–1387.
19. Kelly, L. 1987. The Continuum of Sexual Violence. In *Women*, ed. J. Hanmer and M. Maynard, 46–60. London: Violence and Social Control, Palgrave Macmillan.
20. Esposito, E. 2021. Introduction: Critical Perspectives on GENDER, Politics and Violence. *Journal of Language Aggression and Conflict* 9 (1): 1–20.
21. Leary, M.G. 2007. Self-Produced Child Pornography: The Appropriate Societal Response to Juvenile Self-Sexual Exploitation. *Virginia Journal of Social Policy & the Law* 15: 1–50.
22. Levy, N. 2002. Virtual Child Pornography: The Eroticization of Inequality. *Ethics and Information Technology* 4 (4): 319–323.
23. Lima, D. 2013. Egklimata Misous (Hate Crimes), (in Greek) LLM Dissertation https://ikee.lib.auth.gr/record/134827/files/GRI-2014-12838.pdf . Assessed 15.5.2024
24. Schmid, W.T. 1996. The Definition of Racism. *Journal of Applied Philosophy* 13 (1): 31–40.
25. Lomba, N., Navarra, C. and, Fernandes M. 2021. Combating Gender-based Violence: Cyber violence – European added value assessment. European Parliamentary Research Service, Brussels (https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf). Assessed 15.5.2024
26. Luck, M. 2009. The Gamer's Dilemma: An Analysis of the Arguments for the Moral Distinction Between Virtual Murder and Virtual Pedophilia. *Ethics and Information Technology* 11 (1): 31–36.
27. Manoledakis, I. 2005. *Criminal Law* (in Greek). 7th ed. Thessaloniki: Sakkoulas Publications Athens.
28. Manoledakis, I. 1998. *The Legal Interest* (in Greek). Thessaloniki: Sakkoulas Publications Athens.

29. Martin, A. 2024. The Efficiency of Intersectionality: Labelling the Benefits of a Rights-Based Approach to Interpret Sexual and Gender-Based Crimes. *Human Rights Review.* 25: 1–24.
30. MFHR (Marangopoulos Foundation for Human Rights), (ed Kioupis Dimitris) 2007. Internet Child Pornography (in Greek), Nomiki Vivliothiki, Athens
31. Morgan, L. 2009. The Gamer's Dilemma: An Analysis of the Arguments for the Moral Distinction Between Virtual Murder and Virtual Pedophilia. *Ethics and Information Technology* 11 (1): 31–36.
32. Nair, A. 2010. Real Porn and Pseudo Porn: The Regulatory Road. *International Review of Law, Computers and Technology* 24 (3): 223–232.
33. Neller J. 2023. Hate Crimes as Crimes against Dignity, Papers from the British Criminology Conference, www.britsoccrim.org, Panel Paper ,Vol 22, p 39- 53, Assessed 15.5.2024
34. Olweus, D. 1993. Bullying at School – What we Know & What we Can Do, Blackwell Press, London https://www.getsafeonline.org/personal/articles/online-abuse/, Assessed 15.5.2024.
35. O' Rourke Scott, L. 2024. Technology facilitated domestic abuse (TFDA): a new challenge in the world of gender-based abuse. Houghton F, et al. Sexual, domestic, and gender-based abuse: A collection of experience and opinion, https://research.thea.ie/bitstream/handle/20.500.12065/4708/Sexual%2C%20Domestic%2C%20and%20Gender-based%20Abuse%20A%20collection%20of%20experience%20and%20opinion.pdf?sequence=1&isAllowed=y, Assessed 15.5.2024
36. Ost, S. 2009. *Child Pornography and Sexual Grooming: Legal and Societal Responses*. Cambridge University Press: Cambridge Studies in Law and Society.
37. Ostadtaghizadeh, A., M. Zarei, N. Saniee, and M.A. Rasouli. 2023. Gender-Based Violence Against Women During the COVID-19 Pandemic: Recommendations for Future. *BMC Women's Health* 23 (1): 219.
38. Polyzoidou, V. 2016. *The Criminalization of Child Pornography* (in Greek). Athens: Nomiki Bibliothiki.
39. Report on Gender Equality in EU. 2024. Luxembourg: Publications Office of the European Union, 2024, https://op.europa.eu/en/publication-detail/-/publication/44195827-0906-11ef-a251-01aa75ed71a1/language-en, Assessed 15.5.2024
40. Rogers, M., and P. Ali. 2023. *Gender-Based Violence: A Comprehensive Guide*. Switzerland: Springer.
41. Smith, P.K., H. Cowie, R.F. Olafsson, and A.P. Liefooghe. 2002. Definitions of Bullying: A Comparison of Terms Used, and Age and Gender Differences, in a Fourteen-Country International Comparison. *Child Development* 73 (4): 1119–1133.
42. Speed, A, C. Thomson, and K. Richardson. 2020. Stay Home, Stay Safe, Save Lives? An Analysis of the Impact of COVID-19 on the Ability of Victims of Gender-based Violence to Access Justice. *The Journal of Criminal Law.* 84 (6): 539–572.
43 Uldbjerg, S. 2023. Digital Sexual Assault: Understanding the Non-Consensual Sharing of Sexual Images. In *Gender-Based Violence: A Comprehensive Guide*, ed. M. Rogers and P. Ali, 527–540. Switzerland: Springer.
44. Van der Wilk, A. 2018. Cyber Violence and Hate Speech Online against Women, European Parliament, Policy Department for Citizens'Rights and Constitutional Affairs, Brussels (https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf), Assessed 15.5.2024
45. Watson, S. 2024. Online Abuse of Women: An Interdisciplinary Scoping Review of the Literature. *Feminist Media Studies* 24 (1): 51–69.
46. World Health Organization Report. 2024. https://www.who.int/news-room/fact-sheets/detail/violence-against-women, Assessed 15.5.2024
47. Yar, M. 2006. *Cybercrime and Society*. Sage Publications.
48. Yigang, Q., Weilun, D., Qunfang, W. and Zhicong, L. 2024. Dismantling Gender Blindness in Online Discussion of a Crime/Gender Dichotomy. Proc. ACM Hum. -Comput. Interact. 8, CSCW, Article 01 (March 2024), pp. 31 ff

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Vagia Polyzoidou[1]

✉ Vagia Polyzoidou
polyzoidou.v@unic.ac.cy

[1] University of Nicosia, Nicosia, Cyprus