GLOBAL HUMAN
RIGHTS DEFENCE

Cyberviolence Against Women at the Dawn of the Development of Artificial Intelligence

Anne-Marie Leal

Women's rights – August 2024

Riviervismarkt 5, 2513 AM The Hague, Netherlands

info@ghrd.org

+ 31 62 72 41006

https://www.ghrd.org

CONTENTS

INTRODUCTION

In recent years, the upheaval caused by the digital revolution has led to the transformation of violence against women and girls. The increase in internet access worldwide and the widespread use of digital technologies have fostered the development of a new type of violence, cyberviolence. While women and girls already face daily physical, sexual, and psychological violence in the streets, at home, in public transport, or at their place of study or work, technological advances and the ease of access to the online world have amplified the existing threat, giving rise to cyberviolence. Today, cyberviolence against women and girls adds to the long list of violations of women's rights and contributes to their insecurity by imposing itself as a continuum of violence between virtual and real spheres.

Nowadays, violence against women is the subject of numerous conventions. Physical and psychological gender-based violence has long been addressed by international law. However, cyberviolence has not yet been integrated into these instruments, likely due to its recent emergence. Nevertheless, studies like the one conducted by Plan International in 2020 reveals that 50 percent of women experience more harassment online than in the street and that 58 percent of girls have experienced online harassment (Plan International, 2020). Another survey conducted by Amnesty International confirms those alarming numbers and points out that 46 percent of women claim to have experienced online harassment or misogynistic and sexist harassment (Amnesty International, 2017).

Cyberviolence is a widespread and devastating problem among youth. It is an intersectional form of violence, exhibiting varying patterns and degrees of vulnerability and risk for different groups of women and girls. Violence against women can take many forms, especially in an online environment, including cyberharassment, cyber stalking, trolling, identify theft, non-consensual use of intimate images and videos, threats and calls to violence, sexist hate speech, induction to self-harm, unlawful access to messages or social media accounts, breach of the prohibitions of communication imposed by courts, grooming, or human trafficking. Perpetrators can be partners or ex-partners, colleagues, schoolmates or, as is often the case, anonymous individuals. Some women are particularly exposed, such as women’s rights defenders, journalists, bloggers, video gamers, public figures, and politicians. Violence and abuse online may limit women’s right to express themselves equally, freely, and without fear. These crimes are committed on the internet, through social media and

messaging platforms, and by means of electronic devices. Cyberviolence affects women disproportionately, not only causing them psychological harm and suffering but also deterring them from digital participation in political, social, and cultural life (Council of Europe, n.d).

The complex nature of cyberviolence and its consequences on women's rights are increasingly drawing attention from current scientific and professional practitioners. To gain insight into the nature of cyberviolence, Chapter 1 discusses the legal framework on online gender-based violence (OGBV). Subsequently, Chapter 2 examines different forms of cyberviolence. Finally, Chapter 3 delves into the escalation of cyberviolence due to the advancement in Artificial Intelligence (AI).

LIST OF ABBREVIATIONS

AI - Artificial Intelligence

CEDAW - Convention on the Elimination of All Forms of Discrimination against Women

GREVIO - Group of Experts on Action against Violence against Women and Domestic

EU - European Union

ICCPR - International Covenant on Civil and Political Rights

ICT - Information Communication Technology

LSCSA - Livestreaming of Child Sexual Abuse

OHCHR - Office of the High Commissioner for Human Rights

OGBV - Online Gender Based Violence

1. THE LEGAL FRAMEWORK REGARDING CYBERVIOLENCE AGAINST WOMEN

As cyberviolence against women grows, international legal responses remain inadequate and explores the lack of international legal framework toward online gender violence, highlighting the absence of cohesive global action. In contrast, the progressive development of regional instruments addressing cyberviolence examines regional efforts that, while limited, represent important steps toward addressing this urgent issue.

1.1 THE LACK OF INTERNATIONAL LEGAL FRAMEWORK TOWARD ONLINE-GENDER VIOLENCE

Currently, there is no specific legal framework regulating cyberviolence and thus there is minimal attention given to gender-based cyber violence. However, some of the main legal international instruments can help protect women against this emerging form of violence.

The Convention on the Elimination of all Forms of Discriminations against Women, known as CEDAW, is a principal international instrument in the field of women's rights.. This 1979 Convention defines discrimination against women, condemns its practice, and mandates that State Parties commit to eliminating it through all appropriate measures. Article 1 defines "discrimination against women" as,

> *[...]any distinction, exclusion or restriction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment or exercise by women, irrespective of their marital status, on a basis of equality of men and women, of human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field* (CEDAW, 1979).

Besides that, the Committee on the Elimination of Discrimination against Women issued various recommendations detailing and defining violence against women. General Recommendation No.19 of 1992 elucidated that discrimination against women includes gender-based violence, which is a human rights violation. It is defined as "violence which is directed against a woman because she is a woman or that affects women disproportionately". General Recommendation No. 35 of 2017 suggests that prohibiting gender-based violence against women is now part of customary international law, based on State practice and *opinio juris* as interpreted in General Recommendation No. 19. This Recommendation clarifies that CEDAW applies to gender-based violence in technology-mediated environments. Thus, even without a specific legal definition, OGBV is considered discrimination against women, prohibited by CEDAW and customary international law (CEDAW, 2017). Therefore, despite the absence of a definition of "online gender-based violence" in legally binding instruments, from this analysis it is established that OGBV is included within the concept of discrimination against women, which is expressly prohibited by CEDAW and customary international law.

The International Covenant on Civil and Political Rights (ICCPR) can also be used to tackle the issue of OGBV as Articles 2, 3, and 25 address the rule of non-discrimination, including discrimination on the grounds of sex. Although it does not expressly mention gender-based violence, advocacy for gender-based hatred should similarly be regarded as a violation of human rights.

Additionally, some UN Resolutions address the issue of online violence. In Resolution 68/181, the General Assembly recognises that information-technology-related violations against women "are a growing concern and can be a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights". In Resolution 32/13, the Human Rights Council (HRC) establishes a key understanding for the protection of women on the internet, affirming that people's rights must also be protected online, which is also upheld in HRC Resolution 20/8.

As explained by the Special Rapporteur on violence against women and girls,

> *The view of the Internet and digital technologies as enablers of rights and the digital space as an extension of rights held offline paved the way for discussions on how digital technologies had an impact on women's and girls' rights, specifically with regard to gender-based violence* (OHCHR, 2017, §45).

The HRC also expressly recognises that acts of cyberbullying and cyberstalking are included in the pattern of violence against women, reinforcing the interpretation that OGBV is included within the concepts of discrimination and violence against women. Such an interpretation is also sustained by the Special Rapporteur on violence against women, who affirms that,

> *The definition of online violence against women therefore extends to 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* (OHCHR, 2017, §23).

Furthermore, the UN High Commissioner for Human Rights stressed that "online violence against women must be dealt with in the broader context of offline gender discrimination and violence" (OHCHR, 2017, §57).

From this overview of the international legal framework, it is apparent that despite the lack of a specific binding instrument, women and girls remain entitled to protection from OGBV. As widely established, OGBV must be included within the broader context of gender-based discrimination and violence, allowing for the applicability of relevant international instruments, such as the CEDAW and the ICCPR.

1.2 THE PROGRESSIVE DEVELOPMENT OF REGIONAL INSTRUMENTS ADDRESSING CYBERVIOLENCE

Some regional organisations have also established instruments relating to violence and cyberviolence against women.

The Organisation of American States worked on the elaboration of a convention to eradicate violence against women. As a result of its work, the Inter-American Convention on Prevention, Punishment and Eradication of Violence against Women known as the Belém do Pará Convention was enacted. This Convention is an international treaty signed during a conference held in Belém in Brazil, on June 9th, 1994. The Convention firmly establishes women's right to live a life free from violence and serves as an Inter-American human rights treaty. Even though this Convention represented an important step in the protection of women's rights, it does not mention the digital and online aspect thereof.

Within the African Union, the Protocol of the African Charter establishes the obligation of State Parties to combat all forms of discrimination against women through appropriate legislative, institutional, and other measures (African Union, 2003).

The Europe Continent has the most legislative frameworks tackling cyberviolence against women. Two Council of Europe Conventions mention and cover cyberviolence: the Budapest Convention and the Lanzarote Convention. However, they do not address cyberviolence in a gendered manner.

The landmark Istanbul Convention, also known as the Convention on preventing and combating violence against women and domestic violence, stands as the first instrument in Europe to establish legally binding standards specifically aimed at preventing gender-based violence, protecting victims, and punishing perpetrators. The Convention takes a cross-border approach, extending jurisdiction to cover crimes committed abroad by nationals. It also provides a broader definition of 'gender' as socially constructed roles and attributes, encompassing both men and women as possible victims. It requires State Parties to prohibit psychological violence, stalking, and sexual harassment (Council of Europe, nd).

The Istanbul Convention also established a two-pillar monitoring mechanism, consisting of an independent expert body entitled "The Group of Experts on Action against Violence against Women and Domestic Violence" (GREVIO) and a Committee of the Parties. GREVIO is an organ that prepares reports, conducts country-by-country evaluations, and initiates special urgent inquiry procedures when necessary. In October 2021, GREVIO started taking online violence into account, issuing a General Recommendation on the digital dimension of violence against women. This recommendation is a huge step for repressing and preventing cyberviolence since it,

> *[...]regards the perpetration of violence against women online or with the help of technology as a continuity of the different forms of such violence that affects and exacerbates women and girls experiences of gender-based violence against women to an alarming extent* (GREVIO, 2021).

GREVIO emphasises that "gender-based violence against women in the digital sphere has a serious impact on the lives of women and girls". The body issues recommendations concerning the obligations arising from the Istanbul Convention regarding violence against women and domestic violence in their digital context. Highlighting the three pillars of the Istanbul Convention—prevention, protection, and prosecution—GREVIO offers specific recommendations to address cyberviolence.

The European Union (EU) is also taking significant steps. In April 2024, the European Parliament adopted its first directive on combating violence against women. The provisions of this Directive concerning victims' rights should apply to all individuals subjected to criminal acts constituting violence against women or domestic violence, as defined by Union or national law. That includes "the non-consensual sharing of intimate or manipulated material, cyber stalking, cyber harassment, cyber flashing and cyber incitement", among others. The directive also calls for stronger laws against cyberviolence, better assistance for victims, and steps to prevent rape.

> *It is necessary to provide for harmonised definitions of offences and penalties regarding certain forms of cyber violence where violence is intrinsically linked to the use of information and communication technologies ('ICT') and those technologies are used to significantly amplify the severity of the harmful impact of the offence, thereby changing the characteristics of the offence* (European Parliament, 2024).

Promising initiatives, such as this Directive, are still rare but they offer hope for addressing cyberviolence against women within the legislative framework. The adaptation of legal measures to encompass the online world is encouraging and enhances the protection of women and girls from online violence that continues to grow and develop in alarming ways.

2. THE DIFFERENT FORMS OF CYBERVIOLENCE

Different forms of cyberviolence have emerged since the rise of internet usage and its increased access. This article classifies cyberviolence into eight types, based on extensive research and analysis of digital behaviours and incident conducted by Global Human Rights Defense :

1. Non-consensual sharing of intimate or sexual content;
2. Non-consensual taking of intimate content;
3. Non-consensual taking of intimate or sexual content;
4. Unauthorised use, access or sharing of personal information;
5. Impersonation;
6. Surveillance and Monitoring;
7. Online Gender based hate speech; and
8. Exploitation, coercion, and threats.

2.1 NON CONSENSUAL SHARING OF INTIMATE OR SEXUAL CONTENT

Women are the primary victims of digital violence. Research indicates that 90 percent of cases involving the non-consensual sharing of intimate or sexual images and videos target women. For better insight of this very common form of online violence, the following section examines the offences of "revenge porn" and "porn deepfake".

2.1.1 Revenge porn

Revenge porn refers to the non-consensual release of sexually explicit images or videos of an individual, often disseminated on the internet, typically by an ex-partner or even a hacker. This act is committed without the consent, or even awareness, of the individual and with the often-malicious intent of causing them emotional distress, humiliation, or embarrassment.

Often, society stereotypes this form of cyberviolence as the act of an ex-partner sharing explicit content of their former partner after a breakup, primarily within heterosexual relationships. This perspective confines the issue to a concluded, intimate, sexual, and binary relationship. However, from a literal standpoint, this practice can occur among friends, colleagues, or even strangers, during the course of any relationship, and it can involve more than just two individuals. Furthermore, it is essential to recognise that once these images are shared, they become accessible to a wider audience, who can further distribute the content. Once this cycle begins, it becomes difficult to stop. Revenge porn is often seen as a singular act, but each instance of sharing perpetuates its harmful impact, continuing to victimise the individual involved. Moreover, this social definition in no way addresses the consequences for the victims and does not present this phenomenon as violence but rather as the expression of a negative feeling by the aggressor who needed to relieve some tension or anger and acted

without thinking. As for the victim, it is implied that she was completely at fault for making the mistake to share the content (CVFE, 2018).

This recent trend highlights how rapidly and effortlessly trust can be undermined by new technologies. The disturbing reality is that digital innovations have obscured the line between what we consider private and public. These technologies bridge the physical and virtual realms, creating a continuum of privacy that is far from secure. While women might view sexting and sharing nudes as deeply personal, men can often see no issue in sharing these intimate conversations with other men. This behaviour is often a means of demonstrating their seduction skills and success with women. Among teenagers, a similar gendered pattern emerges: boys frequently exchange or display photos sent by girls to enhance their social standing among peers. These images serve as evidence of their success and help them avoid being labelled as homosexual. This dynamic underscores the problematic ways in which privacy and intimacy are negotiated in the digital age (CVFE, 2018).

In the fight against cyberviolence, it is also important to highlight the implications of using degrading terminology, such as “revenge porn”. Although the terminology “revenge porn” is used in official and unofficial dictionaries to describe the phenomenon, many feminist intellectuals argue its usage is problematic. The use of the term revenge is not adequate for various reasons.

Firstly, it is problematic as it reduces the sharing of intimate and sexual content between two people to mere pornography. It is essential to remember that pornography involves the consensual production of sexual or intimate content by adults when the sharing of intimate and sexual content doesn’t. (CVFE, 2018).

Secondly, framing the non-consensual distribution of intimate material as mere revenge is overly simplistic and narrows the focus to the motives of the perpetrator. The term "revenge" implies that the act is a deserved punishment for the woman, thereby shifting responsibility onto the victim and invoking guilt for the perpetrator's actions. When these images are shared without permission, the victims are often blamed for their involvement in the scenes depicted. However, the non-consensual sharing of intimate or sexual content can occur for various reasons, such as financial gain, misplaced pride, emotional blackmail, seeking attention on social media, or simply to amuse friends. Revenge is clearly not the only motive behind this form of cyberharassment. The definition reflects a double standard linked to the sexist norms present in society. By admitting and justifying anger, it legitimises the act and fails to recognise the victim's suffering (CVFE, 2018).

Recently, this new form of online violence is increasingly being criminalised. Numerous countries, including Belgium, France, and the United Kingdom (UK), have already enacted laws to address “revenge porn”, and the list continues to grow as the issue gains more attention. However, creating a precise legal definition for this offence is challenging, and the complex social dynamics surrounding it add to the difficulty.

2.1.2 Deepfake Pornography

In an era of rapid technological advancement, the misuse of Artificial Intelligence has become a growing concern, notably around the creation of deepfakes. In 2023 alone, approximately 95,000 deepfakes were created, representing a staggering 550 percent increase since 2019. The production of deepfake content is highly selective, often targeting individuals based on gender, nationality, and profession (Home Security Heroes, 2023).

Gender is a significant factor in deepfake targeting. In 2023, 98 percent of all deepfake videos online were pornographic, with 99 percent of the targets being women. The creation of deepfake pornography surged by 464 percent between 2022 and 2023, highlighting a troubling trend. These videos are highly realistic, artificially generated using advanced Artificial Intelligence, particularly deep learning techniques, to superimpose an individual's face onto the body of an actor in a pornographic video, typically without the individual's consent (Home Security Heroes, 2023). Alarmingly, it now takes less than 25 minutes and costs nothing to create a 60-second deepfake pornographic video using just a single clear image of someone's face. The accessibility of such technology means that today, one in three tools can allow the creation of deepfake pornography (Home Security Heroes, 2023).

99%

of the targets of deepfake are women

The proliferation of deepfake technology in the pornography industry demonstrates how technological advancements are often misused to harm women and girls. This is evident from the fact that seven of the top ten pornographic websites host deepfakes, collectively accumulating up to 303,640,207 views. Those significant figures provide insight into the extensive consumption and distribution of deepfake-generated pornographic content (Home Security Heroes, 2023).

Nationality and profession also influence the creation of deepfakes. For instance, South Korean singers and actresses account for 53 percent of individuals featured in deepfake pornography, making them the most targeted group. Additionally, 94 percent of those featured in these videos work in the entertainment industry. Surveys indicate that in some countries, such as the US, nearly half of the male population has viewed deepfake pornography at least once. A survey of 1,522 American males revealed that 74 percent of deepfake users do not feel guilty, believing that it does no harm or that because it is not the real person it is okay. The survey also revealed that 20 percent of participants have considered learning how to create deepfake pornography (Home Security Heroes, 2023).

However, deepfake pornography poses a direct threat to personal integrity and digital well-being. Women affected by this often blame themselves for actions that may have led to the abuse, causing them to withdraw from digital spaces, self-censor, or socially isolate themselves. Similar to cases of non-consensual distribution of sexual images, women and

girls whose images are shared face ongoing humiliation and shame, sometimes leading to suicide. The creation of such content is not just about sexual fantasy but also about power, control, and the humiliation of women. Men's sense of sexual entitlement over women's bodies pervades in internet chat rooms where sexualised deepfakes and tips for their creation are shared. As with all forms of image-based sexual abuse, deepfake pornography aims to silence women and push them off the internet (OAS, n.d).

Some countries are considering extending their laws to criminalise not only the distribution of deepfake porn but also its non-consensual creation. There is an urgent need for responsible use, ethical considerations, and regulatory safeguards to address the evolving challenges posed by deepfake content (The Conversation, 2024).

The European Parliament has taken into account the non-consensual sharing of intimate or and sexual content into its latest Directive. The Directive on combating violence against women and domestic violence of 2024 states that,

> *Member States should, in addition to in-person reporting, provide the possibility to submit complaints online or through other accessible and secure ICT for the reporting of violence against women or domestic violence, at least with regard to the cybercrimes of non-consensual sharing of intimate or manipulated material* (European Parliament, 2024).

The mentioning of this type of violence has large implications for women. According to the Member of European Parliament, Frances Fitzgerald,

> *Under the new legislation, women across Europe will no longer need to fear the unauthorised dissemination of their intimate images, including deep fakes, on the internet. Non-consensual sharing of such images will be recognised as a punishable crime, signalling a major shift in the realm of women's protection online*.

2.2 NON-CONSENSUAL TAKING OF INTIMATE OR SEXUAL CONTENT

The practice of creepshots is a deeply concerning form of cyberviolence that is becoming increasingly prevalent. A creepshot involves a man taking a photo of a woman or girl's buttocks, legs, or cleavage without her consent. This disturbing behaviour has surged recently, with women and girls being photographed in public transport, on the street, and in various public spaces. The non-consensual taking of intimate or sexual images can escalate to even more horrifying acts, such as the recording or capturing of sexual violence, including rape. Sharing these photos or videos online with the intent to shame, stigmatise, or harm the victim is a form of cyberviolence that inflicts severe and devastating consequences on the lives of girls and women.

2.2.1 Upskirting and Downblousing

Digital voyeurism is a form of non-consensual intimate image abuse where perpetrators capture and share unauthorised photos or videos of women's private areas online. These creepshots include practices such as upskirting and downblousing. The upskirting refers to the photographing or filming from a position that permits someone to look up inside of a woman's dress or skirt without her permission. This phenomenon is associated with people who use their phones or small cameras to surreptitiously take pictures of women's skirts (Cambridge Dictionary, n.d. a).

Sometimes, the same malicious practice is called downblousing. This expression describes the taking of unauthorised photographs, but in this case down the top of a woman's blouse. Even if this practice has been mediated a lot in past years, it is still difficult to measure the extent of this phenomenon. Even more when knowing that anyone can be a victim of a creepshot. Practices such as upskirting or downblousing can leave victims feeling extremely vulnerable in public, especially when they are alone. These intrusive actions, where intimate photos are taken without consent, can instil fear and discomfort in victims, making them apprehensive about sharing public spaces. Additionally, the knowledge that someone may have taken intimate images without permission can cause prolonged emotional distress (Police Service, n.d) .

Sextortion can be one of the motives for creepshots. Perpetrators may use these pictures to blackmail victims, threatening to share intimate images online unless they receive money, more intimate images, or sexual favours (EIGE b 2022). Creepshots are frequently used by paparazzi photographers, often capturing images as women step out of cars, known as "crotch shots" (The Guardian, 2009).

In some countries, taking unauthorised photographs beneath a woman's or girl's skirt is treated as a serious offence. In the UK or in France, it is criminalised under the term of "Voyeurism". Recently, Northern Ireland's Assembly included "Upskirting" and "DownBlousing" in its Justice Sexual Offences and Trafficking Victims Act of 2022, imposing up to two years of imprisonment on perpetrators of creepshots. Offenders seeking sexual gratification from this can be placed on the sex offenders' register for up to ten years.

2.2.2 Rape filming

The current state of cyberviolence against women and girls has worsened to the extent that it goes beyond merely sharing intimate content without consent. Men and boys are now recording non-consensual sexual acts and distributing these videos online, often displaying them as a source of pride. In a world where the culture of domination is more prevalent than ever, men still grow up with the belief that they own women and girls' bodies. This long standing mindset views women as sexual and reproductive property that men can possess and exchange. Violence is used as a form of coercive control to maintain patriarchal domination.

The appropriation of women's bodies is a very old phenomenon, dating back almost to prehistoric times. Women are not only women, but they are also seen as territories to demonstrate their dominance to other men, one takes possession of their women's bodies.

This archaic perspective on relationships was highlighted by the infamous case of non-consensual filming of rape known as the Manipur case. In early 2023, a disturbing video emerged showing violence against two naked women who were paraded in the conflict-ridden Indian state of Manipur, shocking the world. The videos, depicting gang rape and sexual assault, went viral on social media and were posted with the explicit intent of drawing global attention to the conflict. Often, women's bodies are used to convey messages and seek attention from other men. In conflicts, the violation of women's bodies highlights who pays the highest price. Women have always been seen as territories whose conquest is considered a win But with the advent of technology, these horrific actions are increasingly going viral and inviting other men to follow that infamous example (The Hindu, 2023).

There is also a rise in the livestreaming of child sexual abuse (LSCSA) as a form of online child sexual exploitation and abuse. Despite its prevalence, limited research has examined this issue. The COVID-19 pandemic has accelerated internet use and familiarity with live streaming services, highlighting the importance of understanding this crime. This crime involves the transmission of LSCSA across national borders over the internet. It can occur in online chat rooms, on social media platforms, and via communication apps. During these live streams, viewers can be passive or active, requesting specific physical or sexual acts to be performed on or by the child. Often, the abusers are the child's own parents, using live streaming as a financial means, as shown in the case of *The Queen vs. Ian Watkins and others, Cardiff Crown Court* of 2013. In this case, singer Ian Watkins was convicted of sexual abuse after encouraging a mother to sexually abuse her child via Skype. As this form of cyberviolence can be exchanged for payment, it can also take place to gratify love interests or satisfy the desires of sexual abusers and viewers (Sherlock and UNODC, n.d).

Filming sexual abuse is not explicitly mentioned in international, regional, and national legal instruments, leaving these forms of online sexual violence inadequately addressed. However, certain legal frameworks may help tackle these forms of violence. For example, Article 2(e) of Directive 2011/92/EU defines "pornographic performance" as,

> *a live exhibition aimed at an audience, including by means of information and communication technology, of […] a child engaged in real or simulated sexually explicit conduct…or the sexual organs of a child for primarily sexual purposes (*Directive 2011/92/EU).

Article 21(1) of the Lanzarote Convention also criminalises "recruiting a child into participating in pornographic performances or causing a child to participate in such performances".

In the Philippines, the Anti-Child Pornography Act of 2009 criminalises child sexual abuse material and can be used to prosecute those involved in live streaming child sexual abuse by making it unlawful to

> *[...] hire, employ, use, persuade, induce, or coerce a child to perform in the creation or production of any form of child pornography…to produce, direct, manufacture, or create any form of child pornography…and to publish, offer, transmit, sell, distribute, broadcast, advertise, promote, export, or import any form of child pornography* (Article 4).

Even though these tools aid in prosecuting specific forms of violence, there is still much to be done to address the non-consensual filming of sexual abuse within legal frameworks. These emerging forms of violence must be incorporated into legal systems as criminal offences, as they devastate lives and have severe consequences for their victims.

2.3 NON-CONSENSUAL RECEIVING OF INTIMATE OR SEXUAL CONTENT

Another form of cyberviolence frequently categorised as cyberharassment is the unauthorised receipt of intimate or sexual images and videos.

2.3.1 Cyber Flashing

Cyberflashing, often referred to as sending "unsolicited dick pics," involves using digital methods such as messaging apps, social media platforms, or peer-to-peer Wi-Fi networks like AirDrop to send explicit images or videos without the recipient's consent. This practice, typically involving men sending unsolicited photos of their genitalia to women, is considered a form of sexual harassment (Cambridge Dictionary, n.d. a).

This troubling trend has been on the rise since the onset of COVID-19. Many women experience cyberflashing as a severe sexual violation and an invasion of their privacy. The unsolicited images can leave recipients feeling shocked, uncomfortable, or humiliated, similar to the feelings women experience when being "flashed" in public. As underlined by the Directive on combating violence against women and domestic violence of 2024, "[c]yberflashing is a common form of intimidating and silencing women" (European Parliament and Council, 2024).

Some women have declared:
"The truth is, no matter how strong I thought I was, he turned me, with a picture, into a weak person, feeling humiliated and with no ability to stand up for myself" (Janay)

"I felt vulnerable ... it was scary not knowing who it was …that they might be looking at me or potentially follow me off the train" (Chloe)

> "I just hate the idea of turning my AirDrop on, even momentarily, and being bombarded again. I hate that men control how I behave" (Sophie)[1]

Cyberflashing can be a one-time incident of exposure or part of ongoing harassment, often involving multiple explicit images or videos. Today, cyberflashing occurs in various ways, women frequently experience it when men nearby use technologies. Some women have even been approached by men in public transportation who then display explicit images on their phones. Cyberflashing has also become common for women using online dating, social media, and other digital platforms, both professionally and personally.

A 2018 YouGov survey found that 41 percent of millennial women (aged 18-36) had received an unsolicited explicit image in their life, with the figure rising to nearly half (47 percent) among women aged 18-24. Reports of cyberflashing to the British Transport Police have been increasing, with 66 cases reported in 2019, compared to 34 the previous year and only three in 2016 (Bowden 2020).

Why do men send unsolicited explicit images? Several reasons have been identified by Clare McGlynn and Kelly Johnson, authors of the book "Cyberflashing: Recognising Harms, Reforming Laws" :

01 **Transactional motives**
Some men send these pictures hoping to receive similar nudes in return or to initiate sexual activity.

02 **Threatening and harassing intentions**
Some men use cyberflashing to create shock and fear, intending to intimidate their victims.

03 **Sexual gratification and exhibitionism reasons:**
Some men seek sexual arousal from exposing themselves to women without their consent.

Many jurisdictions are now recognising cyberflashing as a criminal offence with legal consequences. Countries like Scotland and Ireland have sexual offence legislation broad enough to cover new forms of sexual violence, including cyberflashing. The rise of mobile and digital communication technologies has highlighted the invasive nature of this behaviour and the need for protective measures against it. The next step is to specifically classify cyberflashing as a sexual offence, as current flashing laws in some countries do not adequately address its digital counterpart (Bristol University Press, 2021).

[1] Quotes extracted from 'Cyberflashing: Recognising Harms, Reforming Laws,' a research study conducted by Clare McGlynn and Kelly Johnson.

The EU has taken the next step in this matter, and declared in its latest Directive on combating violence against women and domestic violence that disclosing private information online without consent is prohibited, as is "cyber-flashing" (European Parliament and Council, 2024).

2.4. UNAUTHORISED ACCESS, USE OR SHARING OF PERSONAL INFORMATION

2. 4.1 Doxxing

Technological progress inherently carries significant risks, and one of the threats emerging from today's increasingly digitised lifestyle is "doxxing," which involves publishing private or identifying information about anyone on the internet – typically on social media.

More precisely, doxxing is a deliberate and often malicious act of researching and publicly revealing private or personally identifiable information about an individual, group, or organisation on the internet. This information may include details such as home addresses, phone numbers, email addresses, financial records, and other data that can be used to identify or contact the targeted entity. In the last few years, there have also been cases of personal information being posted on pornographic websites, together with an advertisement that the victim offers sexual services.

Doxxing is typically carried out with the intention of harassment, intimidation, harm, or other malicious purposes and is widely regarded as an unethical and potentially illegal activity. It can happen without evil purposes, but doxxers are usually acting with malicious intent. Like other forms of cyberviolence, doxxing has serious consequences. The information shared online can be exploited by numerous perpetrators in campaigns of harassment and threats, leading to significant psychological trauma. Motives for doxxing may include harassment, exposure, financial harm, or other forms of exploitation of targeted individuals. It can even facilitate physical access to the victim, resulting in further abuse. This could lead to physical harm, such as someone coming to your home or sending threatening items to your address (EIGE, 2022, b).

While anyone can be doxxed, women make up the majority of doxxing victims, as patriarchal structures enable, and oftentimes shield, the men who perpetrate these violations of privacy (AA, 2024). According to a study by Amnesty International in 2017, a quarter of women have been victims of doxxing at least once in their lifetime (Amnesty International, 2017).

Although the term doxxing is not explicitly mentioned in the laws, they do provide, generally, a protection of people's personal information. Some specialists have looked at the framework around digital violence, and declared that we need more digital-specific laws.

Even specialised instruments like GDPR still fail to protect users, especially women, against cyberviolence like doxxing. This is why laws do need to be tailored towards protecting people within the digital space (AA, 2024).

Doxxing has also been covered by the last directive in the EU. The directive states that "Cyberflashing is a common form of intimidating and silencing women" and that,

> *The minimum rules concerning the offence of cyber harassment should also include rules on situations in which the personal information of the victim is made available to the public by means of ICT, without the victim's consent, for the purpose of inciting other persons to cause physical or serious psychological harm to the victim ('doxxing')* (European Union and Council, 2024).

2.5 IMPERSONATION

Impersonation or identity theft is a common form of gendered abuse faced by women. This form of cyberviolence refers to the act of impersonating someone or falsifying a person's identity with the intent to harm, defraud, intimidate, or threaten another individual. Nowadays, it is very easy to impersonate someone or create multiple identities while remaining anonymous (IT for Change, n.d).

Similar to the other types of cyberviolence, women are the first to be targeted. An Australian National University revealed that women are 50 percent more likely than men to be victims of identity theft.

There are two ways for women to face impersonation. The first method occurs when the perpetrator assumes the identity of someone close to or likely to interact with the woman. This tactic is frequently employed to coax women into revealing personal information or sharing intimate images. Subsequently, this information may be exploited for additional offences like doxxing, intimidation, and the unauthorised distribution of intimate images. This tactic is commonly referred to as catfishing *(IT for Change).*

Another method of impersonating a woman involves the perpetrator posing as her to her friends, family, and other public connections, both in person and online, typically with the aim of tarnishing her reputation or credibility. In this form of violence, the perpetrator may send offensive messages and post inflammatory content online, provoking harsh responses, lewd comments, and threats from recipients. This conduct can strain a woman's relationships, subject her to social ridicule, tarnish her reputation, and even result in physical harm offline.

In certain instances of online identity appropriation, perpetrators share manipulated images on fake social media profiles created under the names of victims to damage their reputations within their social circles and attract unwelcome attention and harm. Such acts of

impersonation may compel women to restrict their online presence, including deactivating their social media accounts (IT For change, n.d).

In some countries, impersonation or identity theft is considered a specific offence, such as in France where identity theft through online communication networks is punishable under article 226-4-1 of the Civil Code. However, this is quite rare. More often this type of cyberviolence is covered by general offences but with a reference to 'any means' including ICT means or offences committed in public, such is the case in Czechia, Germany, Estonia or Poland (EIGE 2022, a).

2.6 SURVEILLANCE AND MONITORING

Constant monitoring and surveillance of a person's online and offline activities, or location, constitutes a form of violence that can occur through the installation of spyware on a person' devices or through cyberstalking.

2.6.1 Spyware

Surveillance and monitoring can occur through the malicious deployment of spyware. Spyware is a software program that allows a person to secretly monitor and gather information on another person. This form of cyberviolence involves the unauthorised installation of malware on an individual's devices to clandestinely capture their daily activities, including text messages, emails, photos, and keystrokes or even to freeze, shutdown, or restart a device. These malware programs enable a perpetrator, often referred to as a hacker, to remotely activate a device's camera or microphone, enabling them to track the victim's location, monitor app usage, and intercept calls (OAS, 2024).

The constant monitoring and surveillance of a person's online and offline activities, or location, is a form of violence. This form of violence is a key tactic in intimate partner violence. It has been documented that in 29 percent of cases of domestic or intimate partner violence, the ex-partner uses some type of spyware to track a woman. In most of the cases, hackers geolocalise women by attaching devices to their victims' vehicles, on their phones, and/or by following their victims' location through social media (Women's Aid, 2014).

Documentation of the surveillance impact on spyware victims reveals that control extends beyond the individual cases of women and reflects broader historical and systemic patterns of unequal power dynamics between genders. In Saudi Arabia, communication providers sent SMS notifications to male relatives or 'guardians' whenever their wives or other 'dependents' departed from or arrived in the country. This automated system sparked outrage both domestically and internationally, particularly in a country where women are still considered legal minors. (Privacy international, 2015).

Digital surveillance through spyware is on the rise in various regions of the world. In South Asia, states are increasingly using digital surveillance tactics against female dissidents to silence their voices. Recently, many journalists and human rights defenders in India were subjected to surveillance through the Pegasus spyware. This notorious spyware is employed by numerous governments globally to target and intimidate prominent journalists and activists. According to experts and victims, many women in India, the Middle East, and North Africa, who are presumed targets of government monitoring through Pegasus spyware, now face elevated risks of blackmail or harassment (LSE, 2021).

Spyware software can be installed on computers without the owner's knowledge or even physical access to the device, while cell phone spyware typically necessitates physical access to the phone. In many jurisdictions, installing spyware on another person's devices without their consent for the purpose of stalking is illegal. Furthermore, spyware is invasive and intrusive, posing an increased risk to victims (IACP, 2024).

2.6.2 Cyberstalking

Cyberstalking is a form of digital violence older than the others. At the start of the 21st century, cyberstalking was often romanticised in novels or plays. This form of cyberviolence has not been taken seriously for a long time. The development of the Internet allowed the gathering of information about people and the communication thereof to the target to implicitly or explicitly induce fear. When the problem is raised by intellectuals, society's response is described as making hysteria of a miniscule problem. In fact, the online dimension of stalking was seen as a small problem where victims seldom suffer any real harm (Paul Bocij, 2002).

Cyberstalking describes the use of information and communications technology (ICT), in particular the internet, in order to harass individuals. Acts of cyber stalking can include sending offensive and threatening emails or text messages. Cyberstalking can also refer to watching or spying on a person by means of technology, posting offensive comments about a person on the internet, and sharing intimate photos or videos of a person on the internet or by mobile phone (EIGE, 2022b).

The effects of stalking can be psychologically, economically, and socially devastating on victims. Even if the stalking occurs online, the fear of the victims is real and may persist long after the computer is off. Additionally, cyberstalking can be the first step toward physical stalking. If an individual continues stalking a victim in real life, the consequences of cyberstalking may only become visible later.

Research indicates that cyberstalking predominantly affects women and girls. According to a 2014 survey by the European Union Agency for Fundamental Rights (FRA), five percent of women in the EU had experienced cyberstalking since the age of 15. The survey highlighted significant variation among countries, with Sweden reporting the highest

incidence at 13 percent and Spain the lowest at two percent. Above this, Spain, Bulgaria, Lithuania, Portugal, Romania, and Slovenia each reported a rate of three percent. The survey also revealed that 70 percent of women who experienced cyberstalking had also faced at least one form of physical and/or sexual violence from an intimate partner. While both genders can be victims and perpetrators of stalking, the study found that approximately 80 percent of stalking victims were women, and 86 percent of stalkers were men. Women are more frequently targeted by male (ex) partners and tend to experience greater fear from stalking than men. Men stalked by men report higher levels of fear compared to those stalked by women. Additionally, stalking by (ex) partners tends to be more threatening, intrusive, and violent than stalking by non-partners. Stalking is not always driven by romantic interest and does not always involve innocuous messages. It can also be motivated by hatred, a desire for revenge, a need for power, or even racism (EIGE, 2022b).

7/10

Seven out of ten women who experienced cyberstalking also faced at least one form of physical and/or sexual violence from an intimate partner.

Cyberstalking has been included in the last instruments regarding violence against women. The Istanbul Convention defines it as willfully and repeatedly following or harassing another person in circumstances that would cause a reasonable person to fear injury or death, especially due to express or implied threats.

Legal systems in many jurisdictions recognise stalking as a crime, offering protections such as restraining orders and criminal penalties, as mentioned in the Istanbul Convention. The European Directive of 2024 also tackles this form of online violence and states that

> *The offence of cyber stalking should cover repeated or continuous surveillance, by means of ICT, of the victim without the victim's consent or a legal authorisation. Such surveillance might be enabled by processing the victim's personal data, such as by means of identity theft, by stealing passwords, by hacking the victim's devices, by secretly activating keylogging software to access the victim's private spaces, by installing geo-localisation apps, including stalkerware, or by stealing the victim's devices* (European Parliament and Council of the European Union, 2024).

This definition imposes obligations on states to incorporate these aspects into their legal frameworks stating, "the monitoring of victims, without the victim's consent or authorisation, via technological devices connected through the Internet of Things, such as smart home appliances" (European Parliament and Council of the European Union, 2024).

2.7. ONLINE GENDER-BASED HATE SPEECH

Online gender-based hate speech encompasses content shared through ICT that targets women and/or girls due to their gender or a combination of gender and other factors such as race, age, disability, sexuality, ethnicity, nationality, religion, or profession. This includes material that spreads, incites, promotes, or justifies hatred based on gender or these intersecting identities. Hate speech, whether online or offline, broadly refers to conduct that publicly incites violence or hatred against a group defined by race, religion, nationality, or other characteristics (European Parliament and Council of the European Union, 2024).

The digital realm presents unique challenges for addressing hate speech, including issues of permanence, anonymity, and cross-jurisdictional nature. Online platforms often facilitate full-fledged hate speech campaigns where victims are targeted simultaneously by multiple perpetrators. In the context of gender-based hate speech, examples include body-shaming, slut-shaming, and gender trolling, which undermine women's dignity and safety online.

2.7.1 Gender-shaming

Shaming is primarily a disqualifying discourse about or towards others, often focusing on phenomena related to the body or sexuality. For example, it includes 'slut shaming', 'body shaming', or 'fat shaming'.

Body shaming refers to the act of criticising or mocking someone's physical appearance. It typically involves making negative comments about a person's body size, shape, weight, or other physical attributes. Body shaming can occur in various forms, such as direct verbal insults, derogatory remarks, or through more subtle means like social media posts, memes, or jokes.

The impact of body shaming can be profound, leading to feelings of shame, low self-esteem, and even mental health issues like depression and anxiety in the individuals targeted. It often perpetuates unrealistic beauty standards and reinforces harmful stereotypes about body image. Body shaming can occur across genders and age groups, though it disproportionately affects women and young people due to societal pressures regarding appearance and beauty standards.

Slut shaming is another form of online gender-based hate speech directed toward women and girls, often through social media. It's an act of unfairly judging and stigmatising someone, typically women and girls, based on their appearance, perceived sexual behaviour, or sexual availability. Slut shaming can imply shaming women for their alleged sexual activity in order to embarrass them, damaging their reputation and their sexuality. It may involve the use of photos and/or videos, and demeaning language. This can result in social consequences like rumors, ostracism, or verbal insults such as "slut" or "fag" (OAS, n.d).

Slut shaming can take place in virtual spaces. The rise of social media and new technologies have accentuated this form of violence making it widespread. It can occur online through platforms like social networks, instant messaging, or SMS, greatly expanding its reach and impact. Slut-shaming stems from the misconception that sex, particularly for women, is immoral or shameful. This perpetuates sexist attitudes, sending the message that it's unacceptable for women to embrace their sexuality or enjoy sexual experiences.

Shaming is a long-standing form of gender-based violence that is amplified in the cybersphere: it perpetuates the regulation of women and girls' sexuality and curtails their freedom of speech online (EIGE, 2022b).

2.7.3 Flaming

Flaming is a form of hostile communication that women often encounter during their social media activities. It refers to profanity-laced online interactions marked by insults, negative emotions, and energetic typography, such as capital letters and exclamation marks. Flaming involves deliberately using offensive language to express emotionally charged or contrary statements, typically aimed at provoking a response from another online user. This behaviour frequently occurs in online discussions about controversial topics, such as political, social, cultural, or religious issues. It can be openly misogynistic and is often directed at women with threats or fantasies of sexual violence, or incitement to such violence (EIGE, 2022b).

Flaming, also known as "trash talking," is common in online video games where players use these remarks to provoke their opponents. In 2020, a survey, conducted mainly among girls, underscored the prevalence of toxicity in some video games, revealing that 79 percent of players reported ongoing harassment after matches concluded (Vous, 2022).

Young individuals experiencing online bullying frequently exhibit signs of sadness, frustration, anger, and humiliation. When online flaming escalates from hurtful to potentially illegal or criminal, it is crucial to involve law enforcement for assistance. Whether to contact the police is contingent on the nature of the threats—specifically, threats of violence, bodily harm, death, or the sharing of explicit content like pornography involving children warrant alerting the authorities Lewd language or personal insults directed at a child may also warrant police intervention. The frequency of these incidents is another factor; if the flaming is persistent, increasing in frequency, or spans across multiple online platforms, law enforcement should be notified (Social Media Victim Law Center, 2024).

2.7.4 Gender trolling

Trolling, which involves luring others into futile and endless discussions, is a term used frequently, often in a humorous context. Although not the case, trolling is often perceived as a harmless prank. It is actually a form of cyber harassment that entails posting large quantities of off-topic content, along with inflammatory, insensitive, aggressive, or confusing messages. This behaviour typically occurs on online platforms that encourage debate, such as discussion forums, with the intent of derailing the conversation into a confusing, unsuccessful, and unproductive exchange (EIGE, 2022a).

Regarding other forms of cyberviolence, trolling disproportionately targets women, leading to the creation of the term "gender trolling". This specific type of trolling involves malicious online acts, such as sending offensive emails or social media posts, intended to provoke disputes and elicit angry and distressing responses from the targets (EIGE b, 2022).

Gender trolling has significantly increased since the onset of the COVID-19 pandemic and has evolved to include a wide range of abusive behaviours, from direct insults and verbal attacks to blackmail, deadnaming, doxxing, and even death threats. This form of trolling severely infringes on women's freedom of expression online. According to a report by UN Women, 18 percent of girls who face frequent harassment stop posting content that expresses their opinions and 16 percent alter their online behaviour to avoid harassment (Medium, 2023).

Gender trolling has become a strategic and threatening tool, infiltrating even the political sphere. A recent UNESCO study revealed that 73 percent of female journalists have faced digital attacks in their work, encompassing physical and sexual violence, as well as breaches of digital security. Gender trolling aims to undermine not only the credibility of the women targeted, but also the causes they champion, such as women's equal rights, sexual and reproductive rights, LGBTQIA+ rights, liberal values, and inclusive, diverse democracies. It also seeks to discourage young women from pursuing high-profile careers (Medium, 2023).

Moreover, the current structure of the internet and social media exacerbates gender trolling. Algorithms often promote offensive and misogynistic content to maximise engagement and viral spread (The Guardian, 2023). To combat this form of gender-based violence, there must be more robust legal frameworks that emphasise transparency and hold social media companies accountable for their duty of care when harm arises from their platforms. Some regions are taking steps in this direction. For example, the EU's Digital Services Act (DSA), approved in 2022, mandates platforms like Google and Meta to mitigate the risks their services may pose. It is therefore critical that more countries adopt similar measures to curb gender-based disinformation and online abuse (The Guardian, 2023).

2.8 EXPLOITATION, THREAT, COERCION

Exploitation, threats, and coercion are increasingly facilitated by social media and the internet. Vulnerable children can be targeted within seconds on these platforms, and their anonymity allows perpetrators to extort money more easily than ever before. Online devices also enable individuals to pressure partners into non-consensual activities. Threatening and exploiting individuals is facilitated through ICT, and women and girls are often primary victims to it.

2.8.1 Grooming

Grooming is an act of manipulation of an underage or considerably younger individual, often by an older individual. This form of violence is often predatory and sexual in nature, where an individual uses manipulative behaviour to forge emotional connections with the victim and exert their power over them to exploit them. Grooming does not manifest as a single event, but rather as a process of coercion to prepare the victim in an environment of sexual abuse. It involves manipulative behaviour aimed at obtaining sexual content, such as nude pictures, sexual conversations, and other forms of sexually motivated online interactions. It may also involve phishing for personal information with the aim of establishing physical contact. Grooming begins by making contact with victims, particularly minors, to build a relationship of trust, in which the perpetrators use fake profiles to impersonate someone else and facilitate fake friendships that culminate in extortion (El Pais, 2023). Grooming often occurs in phases to build trust and a relationship with victims: a friendship is formed, followed by relationship building, a risk assessment, and a sexual phase. Groomers may have open profiles, hiding themselves behind fake profiles to pose as children of a certain age and gender (EIGE, 2022b).

Different techniques may be used to achieve grooming. Often, groomers will offer young people advice and a listening ear, along with gifts, compliments, attention, and shared secrets to make them feel special.Part of the 'game' here is for the offender to gain this trust by trying to isolate the young person from their family and friends to create a sense of dependency on them. Isolating the young person from their friends and acquaintances is a common tactic used by offenders to exert power and control over their victims (GSMA, 2017).

Victims are often emotionally isolated from their friends and family, a concerning issue given the easy access children have to the internet today. According to a 2011 study by the EU Kids Online network, which surveyed 25,000 young people across 33 countries, 59 percent of 9-16 year olds are active on social networks, with a quarter of them having public profiles accessible to everyone. Similarly, the 2011 "Children and the Internet" barometer, published by Calysto with the support of La Voix de l'Enfant, found that 39 percent of 13-15 year olds have already made contact with strangers while playing online. Additionally, 23 percent of 11-13 year olds chat with people they have never met on instant messaging platforms, and 15 percent of children in this age group have discovered they were conversing

with an adult when they believed they were talking to someone their own age. As the average age of children accessing the internet continues to decrease year after year, they become increasingly vulnerable targets (Le Journal du Net, 2024).

In some countries, grooming is already considered a criminal offence. For example, in France, since 2007, “the act of an adult making sexual propositions to a minor under fifteen or to a person presenting themselves as such using an electronic means of communication” is punished under Article 227-22-1 of the Penal Code and is subject to two years of imprisonment and a fine of 30,000 euros (Le Journal du Net, 2024).

2.8.2 Sextortion

Sextortion refers to a form of blackmail where an online predator tricks someone into providing nude images or videos and then threatens to distribute this material unless the victim meets their demands, which can include money, more explicit content, or sexual favours. It involves the non-consensual acquisition and/or distribution of sexual images with the intent to harm, humiliate, exploit, or profit from the victim. This form of violence disproportionately affects women and, with a few exceptions, is usually perpetrated by people who identify as men (Cambridge Dictionary, n.d. b).

Unlike more public forms of tech-facilitated abuse, such as image-based sexual abuse, sexual harassment, or revenge porn, sextortion focuses on the threat of releasing images to exert control over the victim. This manipulation leads to significant psychological distress, including fear, shame, and anxiety. The perpetrator's sense of power and the victim's feelings of helplessness are key factors driving the harm caused by sextortion (SAPREA, n.d).

A study by the Royal Melbourne Institute of Technology and Google found that one in seven adults has experienced threats of release of intimate images. Among the 16,000 people surveyed, 14.5 percent reported being victims of image-based abuse, while 4.8 percent admitted to being perpetrators. Almost a third of respondents identified the perpetrator as a former partner (EuroNews, 2024).

In about half of sextortion cases involving minors, the blackmailer follows through with the threat of releasing sensitive content, either posting it online or sharing it with the victim's contacts. Whether the threat is carried out or not, sextortion can have a range of harmful impacts. Victims often experience feelings of helplessness, shame, fear, and loss of control. Many feel trapped and see no way out, leading to severe consequences such as high levels of depression, panic attacks, difficulty eating, self-harm, suicidal thoughts, and in some cases, suicide. These risks can intensify if the sextortionist continues to harass or stalk the victim, creates a fake online profile about them, or encourages them to self-harm. This growing trend of violence places youth at significant risk. A 2018 report by the Federal Bureau of Investigation’s (FBI) Internet Crime Complaint Center noted a 242 percent

increase in emails threatening extortion, most of which were of a sexual nature (SAPREA, n.d).

Sextortion is illegal, with perpetrators facing severe criminal charges. To prevent sextortion, individuals should be cautious about sharing intimate material online, and victims should report incidents and seek support.

2.8.3 Coerced sexting

In recent years, sexting has gained momentum. Today, many people are familiar with sexting and some dictionaries have included its definition, such as the New Oxford Dictionary in 2014.

Sexting involves the creation and sharing of sexually explicit material and can encompass both consensual and non-consensual distribution of images. Several studies have shown that sexting is a common practice among young men and women, who use technology as a means of sexual expression. However, sexting often occurs in contexts where young women and girls face greater social pressure than young men to share sexual and degrading images of their bodies. Conversely, young men and boys are pressured to request, receive, and share these images with their friends to reaffirm their heterosexuality (Arta Dodaj & Kristina Sesar, 2020).

According to Arta Dodaj and Kristina Sesar, they are different types of sexting categories:

01

Relational sexting

Exchange of text, images, and videos of a partner, either naked or semi-naked. When it occurs within a partner relationship, sexting is considered a normal and healthy aspect of sexuality, intimacy, and communication. Typically, this form of sexting is seen as a sign of love or trust towards a partner in an established relationship. It is often used to maintain intimacy when partners are physically separated.

02

Reactive sexting

Opportunistic sexting that refers to the sharing and exchange of intimate and/or sexual images, texts, and videos among adolescents with the primary goal of gaining attention and status among their peers. Unlike intimate sexting within relationships, this form of sexting is driven by a desire for popularity and social validation. Adolescents engaging in opportunistic sexting may knowingly participate despite the risk that sexts could be forwarded beyond their intended audience, potentially leading to wider dissemination without their consent.

03

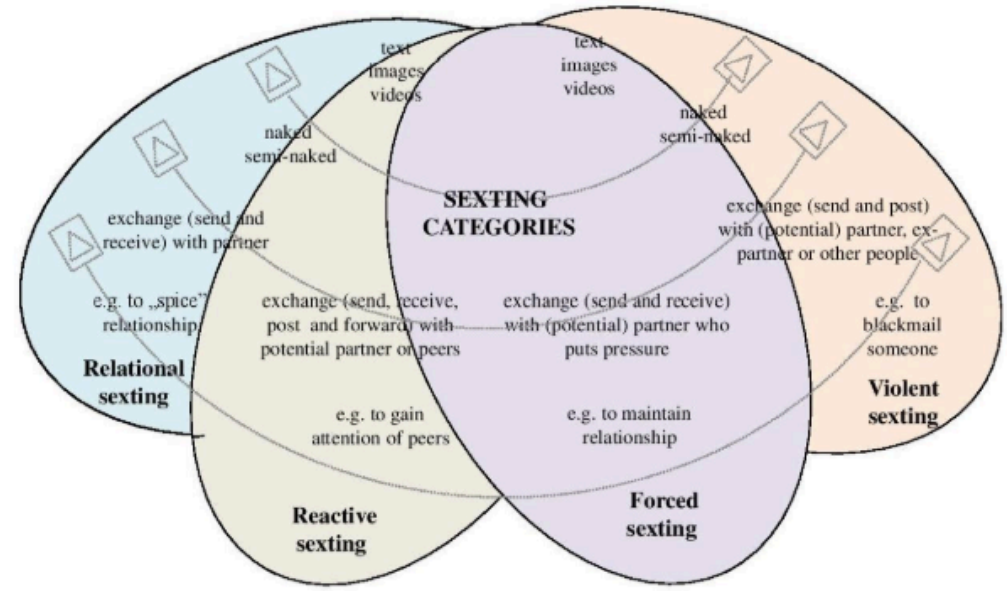
Forced sexting

Sharing of intimate and/or sexual text, images, and videos under pressure from a partner, often to sustain the relationship. In some cases, individuals, typically girls, may consent to 'unwanted' sexting viewing it as a form of 'sexual compliance' or an 'undesirable price' required to maintain a positive relationship dynamic.

04

Violent sexting

Involves the exchange of images, texts, and videos under coercion, often through blackmail. It typically involves adults soliciting sexts from minors or minors engaging in sexting with adults. This behaviour encompasses abusive actions such as sexual abuse, extortion, deception, or the unauthorised sharing of images taken of minors without their knowledge or against their will (Arta Dodaj & Kristina Sesar, 2020).



Source: Arta Dodaj & Kristina Sesa (2020, August), Sexting Categories Consulted on 2024, May 30. Retrieved from https://www.researchgate.net/publication/343650239_Sexting_categories

In many cases, sexting is actually forced sexting, where victims feel coerced into participating due to threats of exposing private information or damaging their reputation. Unlike consensual sexting, forced sexting lacks genuine consent and leads to significant emotional and psychological distress, including feelings of shame, guilt, anxiety, and powerlessness. The fear of explicit content being shared publicly exacerbates these feelings, making the experience profoundly damaging for the victims. Sexting can negatively affect mental health, relationships, and future. It can even have legal consequences (Arta Dodaj & Kristina Sesar, 2020).Sexting involving minors under eighteen is criminalised in many states and often considered child pornography. Sexting is typically classified as a felony and can require sex offender registration for life in some jurisdictions.

3. THE ESCALATION OF CYBER VIOLENCE DUE TO THE ADVANCEMENTS IN ARTIFICIAL INTELLIGENCE

AI is advancing more rapidly than ever before. Often, this development lacks sufficient control, allowing for the emergence of malicious behaviours. Consequently, new and increasingly alarming forms of cyberviolence have surfaced. The use of AI in creating, sharing, and distributing non-consensual intimate content highlights this issue. Now, the fear extends beyond having intimate content shared without consent to the anxiety of having fake content created. Impersonating someone has become effortless with common online tools, and AI is facilitating these criminal behaviours even further.

AI can swiftly and efficiently superimpose someone's face onto existing intimate or pornographic content. One could potentially find their face on a pornographic platform attached to someone else's body simply because an anonymous individual found their face and used AI to manipulate it. AI makes cyberviolence more accessible, quicker, and more pervasive. As evidenced by deepfake pornography involving famous celebrities, this type of cyberviolence affects everyone.

The widespread and nearly universal access to AI enables perpetrators to become increasingly creative in their offences. This has given rise to a new dimension of rape in the digital realm, known as "rape in the metaverse". The metaverse gained popularity in 2021 when Mark Zuckerberg renamed the company that owns Facebook, WhatsApp, and Instagram to “Meta”. It is generally defined as a network of virtual spaces where users can interact.

The European Institute for Gender Equality (EIGE) defines this emerging form of violence as a situation where a person’s avatar, or digital representation of themselves, is subjected to simulated sexual violence by other avatars, particularly in three-dimensional virtual worlds like the metaverse (EIGE 2022, b).

A few months ago, an investigation on rape in the metaverse was started. The British police are investigating a landmark case of an alleged rape in a virtual game after a teenage girl was sexually attacked in the digital world. The girl was reportedly wearing a virtual reality headset and playing an immersive game in the metaverse when her avatar was attacked by several others.

This raises a lot of controversy. Some are questioning whether this constitutes rape and why the girl did not simply turn it off, comparing the situation to other online worlds and video games. One person said sarcastically, “I was killed in [the war video game Call of Duty]... Been waiting for my killer to be brought to justice”. But in fact, there is a slight difference between those two situations. In video games like Call of Duty you can expect to be virtually killed because it is a part of the game, whereas the girl in the metaverse had no reason to expect she would be killed (The Guardian, 2024).

Besides that, Nina Jane Patel, a psychologist that has experienced rape in the metaverse has underlined the fact that,

> *the intensity of experiences in the Metaverse can mirror the emotions felt in the physical world due to the immersive nature of these environments. This can lead to real trauma and psychological distress, akin to those experienced in physical assaults* (Context, 2024).

However, the concept of virtual rape is not entirely new. In 1993, the Village Voice published an article by Julian Dibbell about “a rape in cyberspace”. Yet, today, the question looms larger than ever: are we on the brink of a dark new future? With the advancement of AI, we now have the tools to immerse ourselves fully into digital worlds. Players and online users wearing headphones and virtual headsets make online rape disturbingly real. A researcher from Eko observed that when another avatar touches you in the metaverse, the hand controllers vibrate, creating a disconcerting experience that blurs the lines between real life and the virtual world (Context, 2024).

Experts assert that policing the metaverse presents challenges in defining the crime, establishing jurisdiction, and conducting investigations. Ian Critchley, the lead child protection specialist at the National Police Chiefs' Council, stated that the UK's policing approach must continually evolve to relentlessly pursue predators and protect victims across all online spaces. Currently, it is uncertain if virtual experiences will meet the legal criteria for prosecution. Existing online harassment laws may adapt to protect users in the metaverse, but with the rapid development of AI, significant changes might be on the horizon (Context, 2024).

CONCLUSION

The advent of AI has significantly escalated the complexity and prevalence of cybersexual violence against women. This report has outlined the multifaceted nature of cyberviolence, ranging from non-consensual sharing of intimate images to cyberstalking and online harassment. The immersive environments facilitated by AI, such as the metaverse, blur the lines between virtual and real-world experiences, thereby intensifying the psychological impact on victims.

The current legal framework is insufficient to address the nuanced challenges posed by AI-driven cyberviolence. While international conventions like CEDAW and the ICCPR provide a foundation for combating discrimination and violence against women, there is an urgent need for specific regulations targeting OGBV. The EU's recent directive on combating violence against women is a step in the right direction, emphasising the necessity for harmonised definitions and stringent penalties for cyber offences.

To effectively combat cybersexual violence, a comprehensive approach is required, encompassing legal reforms, technological safeguards, and heightened awareness. Policymakers, tech companies, and civil society must collaborate to create safer digital spaces and ensure that advancements in AI do not perpetuate or exacerbate gender-based violence.

The rapid development of AI presents both challenges and opportunities. It is imperative to leverage AI's potential for positive change while vigilantly safeguarding against its misuse. By doing so, we can work towards a future where digital innovation enhances, rather than undermines, the rights and safety of women.

BIBLIOGRAPHY

AA. (2024, March 22), Doxxing disproportionately impacts women, existing laws falling flat: Expert
Consulted on 2024, May 30. Retrieved from https://www.aa.com.tr/en/science-technology/doxxing-disproportionately-impacts-women-existing-laws-falling-flat-expert/3171670

Amnesty International. (2017, November 20). Amnesty reveals alarming impact of online abuse against women
Consulted on 2024, May 30. Retrieved from https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

Arta Dodaj & Kristina Sesa (2020, August), Sexting Categories
Consulted on 2024, May 30. Retrieved from https://www.researchgate.net/publication/343650239_Sexting_categories

Bristol University Press (2021, March), Cyberflashing: Recognising Harms, Reforming Laws
Consulted on 2024, May 30. Retrieved from https://bristoluniversitypress.co.uk/asset/9542/cyberflashing-policy-briefing-final.pdf

Bowden (2020, February 19): 'Cyberflashing on trains 'largely unreported' despite rise incidents' YahooNews
Consulted on 2024, May 30. Retrieved from https://uk.news.yahoo.com/cyber-flashing-trains-largely-unreported-000100912.html

Cambridge Dictionary (n.d, a), Cyber-flashing
Consulted on 2024, May 30. Retrieved from https://dictionary.cambridge.org/dictionary/english/cyber-flashing

Cambridge Dictionary (n.d, b), Sextorsion
Consulted on 2024, May 30. Retrieved from https://dictionary.cambridge.org/dictionary/english/sextortion

Cambridge Dictionary (n.d, c), Stalking
Consulted on 2024, May 30. Retrieved from https://dictionary.cambridge.org/dictionary/english/stalking

Council of Europe (n,d), Cyber Violence against women
Consulted on 2024, May 30. Retrieved from https://www.coe.int/EN/web/cyberviolence/cyberviolence-against-women

Council of Europe (2011), Convention on preventing and combating violence against women and domestic violence
Consulted on 2024, May 30. Retrieved from

https://rm.coe.int/168008482e

Contex (2024, January 2024), Rape in virtual reality: How to police the metaverse
Consulted on 2024, May 30. Retrieved from https://www.context.news/digital-rights/sex-assault-claims-and-crime-raise-fears-of-new-virtual-wild-west

CVFE (2018, December), Revenge Porn : Critique d'un phénomène social
Consulted on 2024, May 30. Retrieved from https://www.cvfe.be/publications/analyses/170-revenge-porn-critique-d-un-phenomene-social-et-des-mots-pour-le-decrire

El Pais (2023, April 15) A lexicon of cyberviolence: Nine types of online abuse against women that may go unnoticed
Consulted on 2024, May 30. Retrieved from https://english.elpais.com/science-tech/2023-04-14/a-lexicon-of-cyberviolence-nine-types-of-online-abuse-against-women-that-may-go-unnoticed.html#

EIGE (2022, a), Combating Cyber Violence against Women and Girls,
Consulted on 2024, May 30. Retrieved from https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf

EIGE (2022, b) Cyber Violence against Women and Girls
Consulted on 2024, May 30. Retrieved from https://eige.europa.eu/sites/default/files/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf

Euronews (2024, January 4), British police launch first investigation into virtual rape in metaverse
Consulted on 2024, June 13. Retrieved from https://www.euronews.com/next/2024/01/04/british-police-launch-first-investigation-into-virtual-rape-in-metaverse

Euronews (2024, June 13) 'Sextortion': One in seven adults threatened with release of intimate images, study finds
Consulted on 2024, June 13. Retrieved from https://www.euronews.com/next/2024/06/13/sextortion-one-in-seven-adults-threatened-with-release-of-intimate-images-study-finds

European Parliament and Council of the European Union (2024, April 16), Directive on combating violence against women and domestic violence
Consulted on 2024, May 30. Retrieved from

https://www.europarl.europa.eu/doceo/document/A-9-2023-0234-AM-298-298_EN.pdf

European Parliament (2024, April 24), Parliament approves first ever EU rules on combating violence against women
Consulted on 2024, May 30. Retrieved from https://www.europarl.europa.eu/news/en/press-room/20240419IPR20588/parliament-approves-first-ever-eu-rules-on-combating-violence-against-women

European Parliament (2018), Cyber violence and hate speech online against women
Consulted on 2024, May 30. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

GREVIO (2021, October 21) General Recommendation No. 1 on the digital dimension of violence against women
Consulted on 2024, May 30. Retrieved from https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

GSMA (2017), Child Helpline International " Grooming"
Consulted on 2024, May 30. Retrieved from https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2017/03/Grooming_GSMA-CHI_V1_fre-FR.pdf

Home Security Heroes (2024) 2023, State of Deep Fakes: Realities, Threats, and Impact
Consulted on 2024, May 30. Retrieved from https://www.homesecurityheroes.com/state-of-deepfakes/#key-findings

UN General Assembly. (1966, December 16). International Covenant on Civil and Political Rights.
Consulted on 2024, May 30. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

IT for change (n.d) 2.10 Impersonation
Consulted on 2024, May 30. Retrieved from https://projects.itforchange.net/online-violence-gender-and-law-guide/module-2-typologies-of-online-gender-based-offenses-in-law/2-10-impersonation/

Kashvi Chandok (2021,October 25) No safe space for women: The rise in digital surveillance in South Asia
Consulted on 2024, May 30. Retrieved from https://blogs.lse.ac.uk/gender/2021/10/25/no-safe-space-for-women-the-rise-in-digital-surveillance-in-south-asia/

Le Journal du Net (2024, February 2), Le Grooming, un terme méconnu pour une dérive en ligne courante
Consulted on 2024, May 30. Retrieved from https://www.journaldunet.com/ebusiness/le-net/1134690-le-grooming-un-terme-meconnu-pour-une-derive-en-ligne-courante/#:~:text=Cette%20pratique%20a%20un%20nom,%2Dm%C3%AAmes%20des%20enfants…

Medium (2023, December 3), 'Gender Trolling' Has Breached Women's Freedom of Expression Online
Consulted on 2024, May 30. Retrieved from https://medium.com/leveled-legislation/gender-trolling-has-breached-women-s-freedom-of-expression-online-ae3bf5421de6

Merriam Webster Dictionary (n.d) Sextorsion
Consulted on 2024, May 30. Retrieved from https://www.merriam-webster.com/dictionary/sextortion#:~:text=Sextortion%20is%20when%20an%20online,bradfordtoday.ca

OAS (n.d), Online gender-based violence against women and girls: Guide on basic concepts
Consulted on 2024, May 30. Retrieved from https://www.oas.org/en/sms/cicte/docs/Guide-basic-concepts-Online-gender-based-violence-against-women-and-girls.pdf

OHCHR. (2017). *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.* Consulted on 2024, May 30. Retrieved from https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx

Paul Bocij (2002, January), Cyberstalking: Genuine problem or public hysteria?
Consulted on 2024, May 30. Retrieved from https://www.researchgate.net/publication/313001045_Cyberstalking_Genuine_problem_or_public_hysteria

Paul Bocij (2003, January), Cyber stalking: Defining the invasion of cyberspace
Consulted on 2024, May 30. Retrieved from https://www.researchgate.net/publication/285078199_Cyber_stalking_Defining_the_invasion_of_cyberspace

Plan International (2020) Free to be Online ? Girls' and young women's experiences of online harassment

Consulted on 2024, May 30. Retrieved from https://plan-international.org/uploads/2023/06/SOTWGR2020-CommsReport-edition2023-EN.pdf

Police Service of Northern Ireland (n.d), Upskirting and Downblousing
Consulted on 2024, May 30. Retrieved from https://www.psni.police.uk/safety-and-support/online-safety/upskirting-and-downblousing

Privacy International (2015, March 6), International Women's Day: How surveillance is used to assert control
Consulted on 2024, May 30. Retrieved from https://privacyinternational.org/news-analysis/1483/international-womens-day-how-surveillance-used-assert-control

SAPREA (n.d), *What is Sextorsion ?*
Consulted on 2024, May 30. Retrieved from https://saprea.org/blog/what-is-sextortion

Sherloc and UNODC (n.d), Online child sexual exploitation and abuse
Consulted on 2024, May 30. Retrieved from https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html

Social Media Victims Law Center (2024, March 22), What Is Flaming on the Internet?
Consulted on 2024, May 30. Retrieved from https://socialmediavictims.org/cyberbullying/types/flaming/#:~:text=Flaming%20is%20a%20form%20of,common%20places%20for%20flaming%20cyberbullying.

The Conversation (2024, April 9), Deepfake porn: why we need to make it a crime to create it, not just share it
Consulted on 2024, May 30. Retrieved from https://theconversation.com/deepfake-porn-why-we-need-to-make-it-a-crime-to-create-it-not-just-share-it-227177

The Guardian (2024, January 5), A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future?
Consulted on 2024, May 30. Retrieved from https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta

The Guardian (2023, February 17) 'Gender trolling' is curbing women's rights – and making money for digital platforms
Consulted on 2024, May 30. Retrieved from

https://www.theguardian.com/global-development/2023/feb/17/gender-trolling-women-rights-money-digital-platforms-social-media-hate-politics

The Guardian (2009, February 25), 'I felt completely violated'
Consulted on 2024, May 30. Retrieved from
https://www.theguardian.com/lifeandstyle/2009/feb/25/women-upskirting

UN General Assembly. (1979, December 18). Convention on the Elimination of All Forms of Discrimination Against Women.
Consulted on 2024, May 30. Retrieved from
https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women

Vous (2022, August 20), Comptes « fisha », doxxing, flaming : petit lexique du harcèlement en ligne
Consulted on 2024, May 30. Retrieved from
https://vousparmacif.macif.fr/comptes-fisha-doxxing-flaming-petit-lexique-harcelement-en-ligne

West Yorkshire Police. (n.d). *"Cyber-flashing"*
Consulted on 2024, May 30. Retrieved from
https://www.westyorkshire.police.uk/ask-the-police/question/Q989#:~:text=Cyber%2Dflashing%20is%20the%20sending,Fi%20networks%2C%20such%20as%20AirDrop