Report on Cyber Violence Against Women

POLICY OVERVIEW AND
RECOMMENDATIONS

SEPTEMBER 2024

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. The European Union can not be held responsible for them.

CREDITS

Virginia Dalla Pozza
Main Author

Iliana Balabanova
EWL President

Mary Collins
EWL Secretary General

Veronica Zaboia
Project Coordination

Maria João Faustino
Scientific Contribution

Yvonne Redin
Graphic Design

Laura Kaun, Irene Rosales, Alexia Fafara, Veronica Zaboia, Maria João Faustino
Contributors

Funded by
the European Union

EUROPEAN WOMEN'S
LOBBY
EUROPEEN DES FEMMES

TABLE OF CONTENTS

TABLE OF CONTENTS

ACRONYMS

AI
Artificial intelligence

CoE
Council of Europe

CVAWG
Cyber violence against women and girls

CVAW
Cyber violence against women

DV
Domestic violence

DSA
Digital Service Act

DSC
Digital service coordinator

ECHR
European Convention on Human Rights

EWL
European Women's Lobby

EIGE
European Institute for Gender Equality

EPRS
European Parliament Research Service

FRA
European Union Agency for fundamental rights

GBV
Gender-based violence

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

ICT
Information communication technology

IPV
Intimate partner violence

SDGs
Sustainable Development Goals

TFV
Technological-facilitated violence

TF VAW
Technological-facilitated violence against women

UN
United Nations

VAW
Violence against women

VLOPs
Very large online platforms

VLOSEs
Very large online search engines

VRD
Victims' Rights Directive

NOTES ON TERMINOLOGY: Section 2.2 of this Report provides an overview of the terminology used to define cyber violence against women (CVAW). While the term CVAW is mostly used in the EU context and has, thus, been preferred in this Report, the concepts of technological-facilitated violence (TFV), technological-facilitated violence against women (TF VAW) and/or online violence have also been used when the sources explicitly referred to these terms. Moreover, in line with EWL's feminist approach and values, the term sexual digital forgeries has been preferred to 'deepfakes'.

The term 'deepfakes' is a portmanteau of 'deep-learning' (referring to a method of artificial intelligence) and 'fake'; the latter entered the public jargon in 2017 when a perpetrator used that name on the website Reddit to refer to images and video he manipulated with AI to insert female celebrities' faces into pornographic videos without their consent.[1] Considering that the word has been coined by a perpetrator, in order to better reflect the victims' and the feminist perspective, the EWL prefers to use the terms 'sexual digital forgeries' and 'digital forgeries' as suggested by Mary Anne Franks.[2] However, for the sake of clarity and in order to respect the original source of information, in some cases we kept in this Report the reference to 'deepfakes' in brackets.

I. Introduction

1. FOREWORD

Violence against women (VAW) is a manifestation of men's domination and unequal power over women to silence their voices, control their lives, bodies and sexuality and *'keep them in their place'*.

Male VAW takes many forms and is part of a continuum of violence embedded in the patriarchal society. Male VAW is intrinsic to a culture of sexism, coupled with all forms of gender-based inequalities; these include women's poverty, gender pay and pension gaps, unequal participation in political life and all areas of leadership, unequal access to public services: health, including sexual and reproductive rights, housing, transport, media, etc. and economic independence to enable women to make real choices in their lives.

There is not one single country in the world where women and girls are free from male violence and not a single area in any woman's life where she is not exposed to the threat or reality of acts of male violence.

The digital world/culture is no exception to this rule. One in three women in Europe has experienced physical, psychological, emotional and/or sexual violence since the age of 15, representing an astounding 62 million women.[3] It is likely that this is only the tip of the iceberg. While it is difficult to determine with precision the actual prevalence of online violence against women and girls, data provided by EIGE[4] estimates that one in ten women have already experienced a form of cyber violence since the age of 15. Moreover, in the past ten years, there has been an exponential explosion of cyber violence against women and girls (CVAWG).

CVAWG can take many forms and expressions. These are evolving extremely rapidly in a fast changing virtual (and real) world, through social media and more recently artificial intelligence, which have been and continue to be an invasive space for women and girls. Identifying, recognising and properly naming these forms is a fundamental step to eradicate CVAWG.

Male VAW thrives through impunity, and this is often exacerbated when perpetrated online. Seeking justice to combat CVAW requires robust international legal and policy measures, as the virtual space knows no geographical boundaries. A holistic approach that encompasses legal tools to prevent CV and effectively protect victims, accountability of tech companies, as well as coordinated responses to challenge sexism and cultural norms on men's dominance over women, are needed. The porn industry must also be tackled. It is never women's responsibility to prevent male VAW.

The recently adopted EU Directive on combating VAW and domestic violence[5], provides for harmonised definitions of offences and penalties regarding certain forms of CV, namely:

- Non-consensual sharing of intimate or manipulated material (article 5)
- Cyber stalking (article 6)
- Cyber harassment (article 7)
- Cyber incitement to violence or hatred (article 8)

It also provides for penalties (article 10) and aggravating circumstances (article 11).

While this is a very good step in the right direction, it will require close effective monitoring of the transposition of this Directive, for which this report also provides recommendations.

Leaving no girl or woman behind takes all its meaning in combating male VAW, both online and offline, to ensure that all women and girls across generations know that it is their right to live free from male violence. This report aims to contribute to this. Besides, the report aims to ensure that all women and girls can identify with the different forms of CV to which they are, or potentially can be, exposed.

Ending all forms of VAW is a prerequisite to achieving effective equality between women and men.

This report is embedded in the European Women's Lobby's (EWL) mission, vision and principles: women's rights are human rights, solidarity, autonomy, participation and inclusion.

2. BACKGROUND

Technology and digitalization shape our daily life in numerous ways, from the way we communicate and work to the way we shop and entertain ourselves. **Technology and digitalization** play an important role in women' lives too, they could be **crucial tools for women's empowerment**. They could enhance women's opportunities to access information, knowledge and services; to connect with others; and to advocate for their rights.[6] The connection between technology and women's rights is embedded in the Sustainable Development Goals 5 (SDG 5),[7] which include a specific target on utilizing technology and ICTs to realize women's and girls' empowerment.

Despite these benefits, in a context of increasing violence against women (VAW), technology also has some drawbacks; **it can offer perpetrators the opportunity to commit VAW in an anonymous manner**.[8] The digital arena has become a breeding ground for violent discourses as well as other forms of cyber violence against women (CVAW) with anonymity and impunity. The situation has become even worse during the COVID-19 pandemic, which contributed to an increasing reliance on digital technologies.[9]

VAW in an online environment can take several forms, among others: cyber harassment, cyber stalking, non-consensual sharing of intimate material, hate speech etc. The Internet has also been used to spread online hate communities against women (the manosphere) who foster a miso-gynistic culture, antifeminist and sexist beliefs. Similarly, pornographic platforms contribute to the proliferation of a patriarchal culture that justifies VAW. Such forms and the means to commit CVAW are in **continuous evolution** in parallel with the development and increased use of new technologies. **Perpetrators of CVAW** can be the victims' partners or ex-partners, family members, friends or anonymous individuals.

The **short and long-term impacts on female survivors are particularly severe**. Victims often withdraw from the digital sphere, silencing and isolating themselves and losing opportunities to build their education, professional career and support networks.[10]

Advancements in technology and related abuses online occur at a much faster pace than States and lawmakers are able to respond. In the lack of adequate and prompt responses, the forms, intensity and spaces of CVAW have been expanding, contributing to women's growing feelings of unsafety, discouragement and withdrawal from online public spaces.[11] In the context outlined above, the European Women's Lobby (EWL) has commissioned this Report with the aim to provide recommendations to policy makers and other stakeholders to effectively counter CVAW. While the topic has been extensively investigated by several studies, the **need for up-to-date knowledge** is paramount in

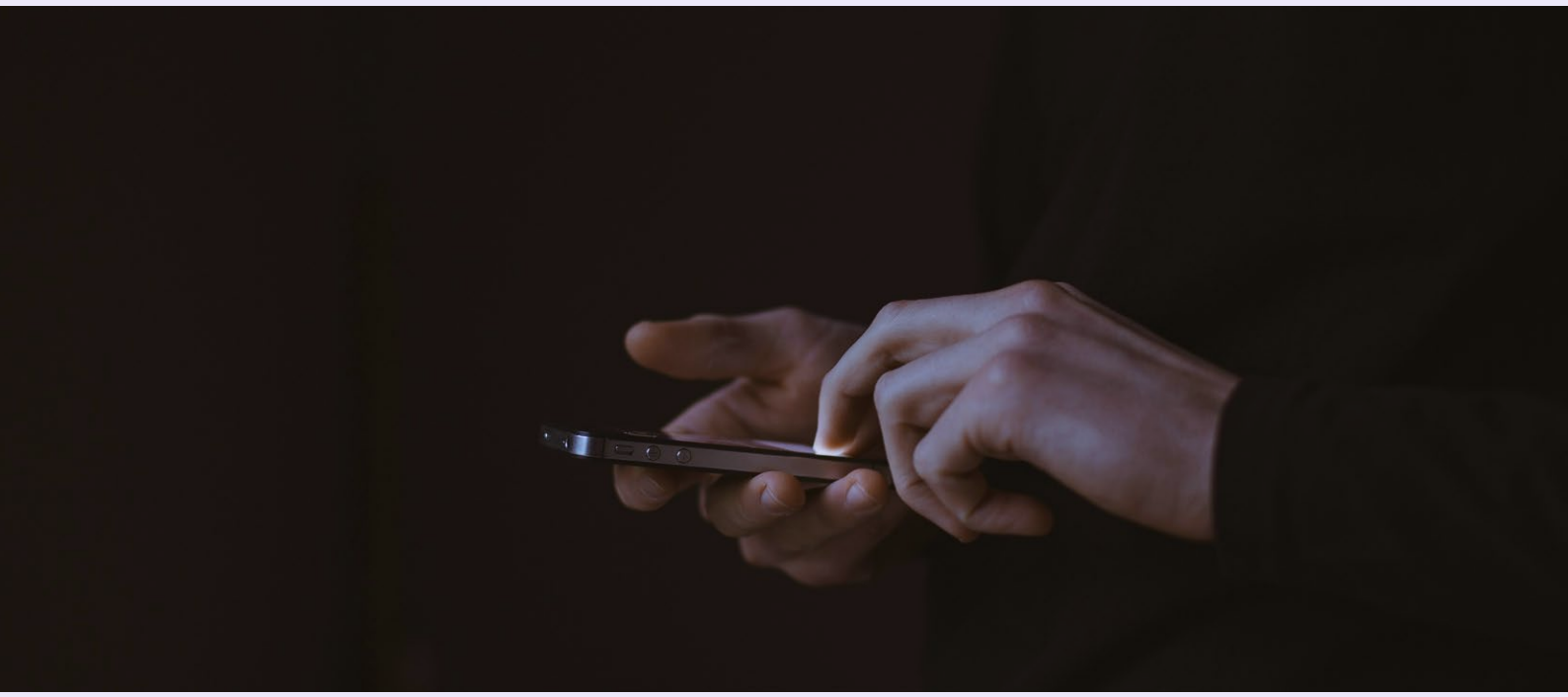
this field considering the continuous evolutions of CVAW and its manifestations, in parallel with the changing technologies used to commit it.

The Report investigates, among others, the forms of CVAW that have become increasingly threatening to women. In particular, the Report has **five main objectives**:

1. Provide insights into CVAW and its key characteristics.
2. Examine the legal and policy framework on CVAW at international, EU and national level;
3. Identify key challenges in this area;
4. Select examples of good practices on how to address CVAW;
5. Put forward recommendations for the EU institutions and Member States to effectively tackle CVAW.

In line with the principles outlined in Section 1.1, the Report, taking a feminist approach, highlights the **gender dimension of CVAW** and includes **survivors' voices** to shed light on their experiences (see Section 2.8).

Since 2017, **the EWL has been working to raise awareness and prevent CVAW**. A first project carried out in 2017 led to the publication of the #HerNetHerRights report & Resource Pack[12] aiming at analysing the state of CVAW in Europe of the time. Following up on the report, the EWL organised several cycles of trainings on CVAW targeting women in politics who candidated for elections in order to raise awareness about CVAW and propose tools and suggestions on how to take action and eradicate it. Such trainings were prepared for the 2019 and 2024 EU elections, as well as for national elections in countries such as Austria, Bulgaria, Finland, Italy, Romania, Sweden, Denmark and Turkey.

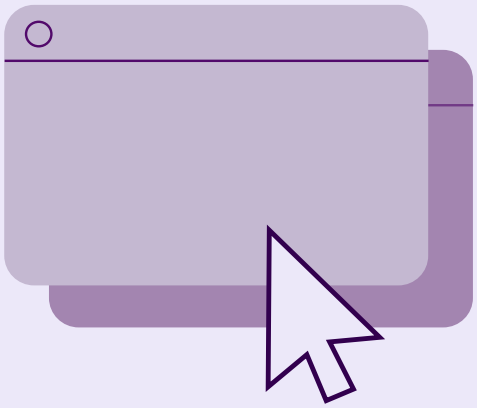


3. CONCEPTUAL FRAMEWORK

The following research methods were used for this Report:

- **Desk research**: desk research covered a broad range of materials including studies, reports, articles, websites, databases and projects on CVAW issued by international, EU and national actors.

- **Legal & policy review**: a detailed review of legal and policy documents was conducted to map legislative and policy instruments that may be applicable to CVAW. The review encompassed documents at international, EU and national level.



- **Stakeholder consultation**: in order to further explore specific themes of the Report, five key stakeholders were consulted. Stakeholders from different categories (academia, institutions, NGOs) were selected in collaboration with EWL. All consultations were carried out through video-calls, using semi-structured interview questions to allow the interviewees to openly discuss the topics of relevance. Long discussions (of around 45-60 minutes) were carried out in the month of February for the specific objectives of:

  - Ensuring that the research topics of the Report were comprehensive and did not neglect important aspects of CVAW;

  - Exploring the latest trends and manifestations of CVAW, on which information may not yet be published;

  - Gathering stakeholders' views on challenges, good practices and recommendations to tackle CVAW. The stakeholder consultation guaranteed that the content produced in this report is as comprehensive and recent as possible.

The findings from the above-mentioned activities were analysed and triangulated to identify recurring themes, gaps and/or inaccuracies. Moreover, the Report was subject to a scrupulous review by the EWL.

4. STRUCTURE OF THE REPORT

This report is structured into six chapters:

CHAPTER ONE

Contains background information on CVAW and explains the objective of the Report, the methodology used and the structure of the report.

CHAPTER TWO

Provides an overview of the phenomenon of CVAW and is structured around key questions.

CHAPTER THREE

Outlines the legal and policy framework on CVAW at international, EU and national level.

CHAPTER FOUR

Discusses the key challenges in this area.

CHAPTER FIVE

Presents examples of good practices on combating CVAW.

CHAPTER SIX

Puts forward recommendations to tackle CVAW for both EU institutions and Member States.

II. Cyber Violence Against women

This section aims to provide an exploration of CVAW in a concise manner by replying to a range of key questions about: what CVAW is and how it is defined, the main forms of CVAW, its prevalence, the space where it mostly occurs, the most likely victims and perpetrators as well as the short and long term consequences on women. The information has been collected through a thorough desk research and stakeholder consultation.

1. WHAT IS CYBER VIOLENCE AGAINST WOMEN?

Cyber-violence is the use of online and communication technologies to cause, facilitate or threaten violence against individuals.[13] '**Cyber violence against women**' or '**Gender-based cyber-violence**' are some of the several umbrella terms used to describe the dimension of violence enabled by internet, emails, smartphones and social media platforms.[14] As explained in Section 2.2, the definitions of CV vary considerably not only across countries but also across key actors in this field, with the result of having different terminologies from one organisation to another.

Despite the great variance in terms, CV has some specific features[15] that distinguish it from other forms of offline violence and make it particularly dangerous for women:

- **It has a broad reach, transmission and speed**: the easy and rapid dissemination of content through multiple platforms and social media make it difficult to control the type of information that is disseminated via digital means;

- **It offers a lack of inhibition**: the enhanced anonymity offered by digital and virtual spaces through encryption and privacy protocols allows users to behave with anonymity and impunity. This makes the identification of perpetrators particularly challenging;

- **It is hard to eliminate**: the violent content becomes persistent, difficult to remove and, therefore, re-traumatizing for the victims.

Other key aspects of CV that need to be taken into account are: its **gender dimension**, its **root causes grounded on structural gender inequalities** and the fact that it is part of a **wider continuum of VAW**.

As highlighted by UN Women,[16] while men can also experience online violence and abuse, **women and girls are more likely to experience unique forms of gendered violence in digital contexts**, reflecting a similar pattern to VAW and girls in the physical world. Likewise, according to EIGE,[17] CV is an emerging **new dimension of GBV**. The gender nature of CV is recognised also by GREVIO[18] according to which women are more likely to experience sustained physical, psychological or emotional abuse (both offline and online) which has serious impacts on women's lives (see Section 2.8).

Several studies report that **women and girls are over-represented as victims of CV**. For example, a 2021 survey by the Pew Research Center found that although men were slightly more likely than women to experience 'mild' forms of cyber harassment (e.g. name-calling and embarrassment), women disproportionately experienced severe forms of CV, such as cyber stalking and online sexual harassment.[19] Along the same lines, international research indicates that, with the rise in the use of digital technologies due to the COVID-19 pandemic, women and girls are more likely than men to become victims of serious forms of CV and the impact on their lives is far more traumatic [20] (see Section 2.6).

CV is rooted in the same context of women's inequality as offline VAW.[21] Digital spaces reinforce and intensify **systemic structural gender inequalities** as well as patterns of harmful masculinities that drive all forms of VAW. Cultural and social norms, reinforcing male power, trivialise and excuse both offline and online violence. As a result, survivors are stigmatised and patterns of violence persist.[22] Moreover, as mentioned above, the specific features of digital spaces create a particularly conducive environment for VAW, including the scale, speed, and ease of online communications. Anonymity, combined with automation and impunity, create a fertile ground for CVAW.

Besides, as stressed by the Advisory Committee on Equal Opportunities for Women and Men,[23] CV is part of a **continuum of violence against women**;[24] it does not exist in a vacuum, rather, it both stems from and sustains multiple forms of offline violence. Indeed, online violence and offline violence are often interconnected and/or intertwined.[25] In this regard, GREVIO draws attention to the need to acknowledge digital VAW as a continuum of violence against women offline, which forms part of GBV against women.[26] Likewise, the United Nations (UN) [27] point out that although the patterns and forms of VAW in digital spaces can be unique, they are part of the continuum of multiple, recurring and interrelated forms of violence across online and offline spaces. Many forms of violence occurring offline are replicated and intensified in digital spaces. As argued by academics,[28] distinctions between 'offline' and 'online' behaviours are not reflective of women's experiences of CV. Women commonly experience violence and abuse online and offline, such as stalking or harassment, not in separate categories, but as a whole experience.

2. HOW IS CYBER VIOLENCE AGAINST WOMEN DEFINED?

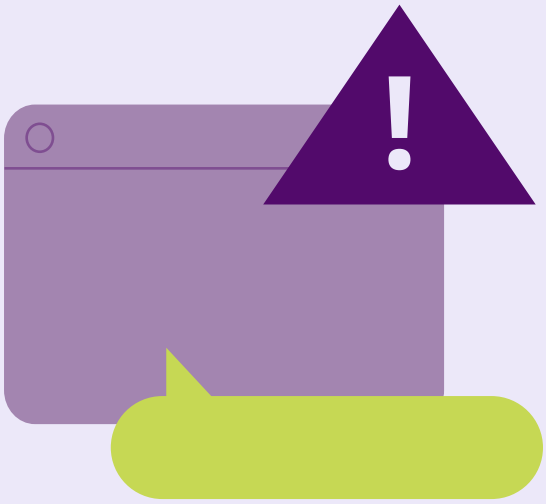
One of the obstacles pointed out by various stakeholders in the field, including the consulted experts, is the **lack of a common definition of CV**. Different key players use different terms. For example, **EU organisations** (e.g. EIGE, the Advisory Committee on Equal Opportunities for Women and Men) tend to refer to 'cyber violence' whereas academic literature prefers 'online or digital violence'.

At international level, **GREVIO** uses the concept of 'the digital dimension of violence against women'.[29] The latter encompasses a wide range of behaviours that fall under the definition of VAW set out in Article 3a of the Istanbul Convention.[30] Non-consensual image or video sharing, coercion and threats, including rape threats, sexualised bullying and other forms of intimidation, online sexual harassment, impersonation, online stalking or stalking via the Internet of Things are covered by this definition.

At UN level, the **Special Rapporteur on VAW** refers 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'.[31] The term 'technological-facilitated violence' (TFV) is preferred by the **UN Women**.[32] In this regard, the UN Women expert group defines 'technology-facilitated VAW' as 'any act, that is committed, assisted, aggravated or amplified by the use of ICTs or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements'. In this definition, 'ICT' is an umbrella term that includes mobile phones, the Internet, social media platforms, computer games, text messaging, email and other related technologies.

At the **national level**, as pointed out by EIGE,[33] there is a high degree of variety, overlap and disharmony of legal and statistical definitions across Member States.

Overall, **differences in terminology reflect differences in the conceptual approach** towards online violence, its scope, and which specific forms are covered.[34] While narrow conceptualisations present the advantage of allowing global comparisons, they may overlook the many ways in which ICTs and other digital tools impact all women.[35] Broader conceptualisations are, indeed, needed to ensure that the definition of CV is as comprehensive as possible.



According to GREVIO,[36] different terms are used interchangeably or inaccurately, creating a fragmentation that is reinforced by the diversity of aims and perspectives of the different stakeholders. Many terms in use do not cover the full range of behaviours, nor do they highlight the gender pattern in the abuse.

The lack of harmonised definitions has **several implications**. The absence of agreed definitions and methodologies for measuring CV, together with high underreporting, make it hard to capture the true extent of the problem globally as well as to identify any regional variations[37] (see Section 4.5).

3. WHAT ARE THE MAIN FORMS OF CYBER VIOLENCE AGAINST WOMEN?

The sections below present the main forms of CVAW; these should not be considered as separate categories as each form of CV is interlinked to other forms, both offline and online, in line with the concept of continuum of violence (see Section 2.1).

3.1 THE MOST PREVALENT FORMS

The forms and patterns of CVAW continue to evolve and multiply as technology advances in a context of increasing digitalization, accelerated by COVID-19. CVAW can take many forms. Data on the most prevalent forms vary from one study to another, depending on the methodology and geographical area considered as well as the definitions of CV used. Nonetheless, it seems that **cyber harassment, cyber stalking, non-consensual sharing of intimate material and hate speech** are the most widespread forms. According to a 2021 global report, the most common forms of violence reported globally include: misinformation and defamation (67%), cyber harassment (66%), hate speech (65%), impersonation (63%), hacking and stalking (63%), astroturfing (a coordinated effort to concurrently share damaging content across platforms, (58%), video and image-based abuse (57%), doxing (55%), violent threats (52%), and unwanted images or sexually explicit content (43%). Among women who have experienced TF VAW in Eastern European countries and Central Asia, the most prevalent forms include: receiving unwanted or offensive content or messages (39.7%), receiving inappropriate sexual advances or content on social networking (30%) and hacking women's accounts and web pages (25.4%).

3.2 INCREASINGLY THREATENING FORMS

Given the incessant evolution of digital technologies, increasingly threatening **forms and modes** of CVAW are expected to emerge. Among these forms, the Report focuses on patterns of CVAW that are proliferating through the **use of artificial intelligence, virtual reality and online gaming**; these forms were highlighted by the consulted stakeholders as more and more dangerous to women and confirmed by the findings of desk research. Other forms exist and will continue to emerge with advancements in technology.

The table on the next page lists **some of the technologies**[41] that are used to commit increasingly dangerous forms of CVAW.

Some of the technologies used to commit increasingly dangerous forms of CVAW	
Artificial intelligence	Artificial intelligence is a field that combines computer science and robust data sets, to enable problem-solving. It also encompasses subfields of machine learning and deep learning, which are frequently mentioned in conjunction with artificial intelligence. Artificial intelligence seeks to create expert systems which make predictions or classifications based on input data, and leverages computers and machines to mimic the problem-solving and decision- making capabilities of the human mind. Artificial intelligence has been increasingly used to create sexual digital forgeries (known as 'deepfakes') and other forms of CVAW (see below).
Drone	In technological terms, a drone is an unmanned aircraft, it is a flying robot that can be remotely controlled or fly autonomously through software-controlled flight plans in their embedded systems, working in conjunction with on-board sensors and GPS. Drones are now used in a wide range of civilian roles ranging from search and rescue, surveillance, traffic monitoring, weather monitoring etc. Perpetrators are using drones to stalk victims in new age of technology.
Geolocation	Geolocation is a feature on a device that is able to deduce its geographical position through GPS signals or other forms of connectivity. Cyberstalking, especially in the context of intimate partner violence (IPV), has been perpetrated by using geolocation and GPS technologies to monitor and track a victim's whereabouts.
GPS	GPS tracking is the surveillance of location through use of the Global Positioning System (GPS) to track the location of an entity or object remotely. The technology can pinpoint longitude, latitude, ground speed and course direction of the target. GPS devices in smartphones and other mobile devices are often used to track employee location, for example. Privacy advocates warn that the technology can also make it possible for advertisers, governments, hackers and cyberstalkers to track users through their mobile devices. As explained above, cyberstalking, especially in the context of IPV, has been perpetrated by using geolocation and GPS technologies to monitor and track a victim's whereabouts.
Spyware/ Stalkerware	Spyware is software, usually in the form of an app, downloaded onto someone's phone or device and used to track the activities of that device. Spyware is considered stalkerware in the context of domestic violence. Spyware has been used in the context of IPV.

Artificial intelligence and sexual digital forgeries (commonly known as 'deepfakes')

The connection between **artificial intelligence and gender bias** has been increasingly explored in the academic field. This aspect concerns CVAW given that gender stereotypes are among the root causes of CVAW. Research shows that AI systems created by tech giants have large gender and racial bias.[42] Gender bias in these systems is pervasive, it reinforces and amplifies existing harmful gender stereotypes and prejudices. This is linked to the fact that only 22% of professionals in AI and data science fields are women (see Section 4.6). Societal biases linked to gender roles are embedded in social programmes and services through automated decision-making. Algorithms and devices have, thus, the potential to spread and reinforce harmful gender stereotypes.[43]

Another aspect linked to the use of AI is the sharp **increase in sexual digital forgeries, commonly known as 'deepfakes'**.

As reported by EPRS' 2021 study, AI tools to create sexual digital forgeries are developing rapidly and are becoming cheaper, more sophisticated and accessible to users day by day.[44] The World Economic Forum's Global Risks Report 2024[45] has ranked misinformation primarily driven by 'deepfakes', as the most severe global short-term risk the world faces in the next two years. Despite detection tools, these technological solutions are not able to keep at pace with the rapidly advancing capabilities of deepfake algorithms. Legal systems and governments are struggling to regulate this swift advancement of digital deception.[46]

Digital forgeries or 'deepfakes' are defined as 'manipulated or synthetic audio or visual media that seem authentic, and which feature people that appear to say or do something they have never said or done, produced using artificial intelligence techniques, including machine learning and deep learning'.[47] Digital forgeries are a subset of a broader category of AI-generated 'synthetic media', which not only includes video and audio, but also photos and text. There are various synthetic media that are powered by AI, the main categories are: digitally forged videos, voice cloning (voice cloning technology enables computers to create an imitation of a human voice) and text synthesis (text synthesis technology is used in the context of digital forgeries to generate texts that imitate the unique speaking style of a target).[48]

The consequences of digital forgeries are alarming: they may have negative repercussions at an individual, organisational and societal level. They can cause psychological, financial and societal harm. Psychological harm includes: sextortion, defamation, intimidation, bullying, undermining trust. Financial harm includes: extortion, identity theft, fraud, reputational damage etc. Societal harm includes: news media manipulation, damage to economic stability, damage to the justice system, damage to democracy, manipulation of elections, damage to national security etc.[49]

The gender dimension of the phenomenon is well evidenced. Research shows that women are at increased risk of defamation, intimidation and extortion, as deepfake technologies are currently predominantly used to swap the faces of victims with those of women in sexual abuse

videos. Digital sexual forgeries almost exclusively target women.[51]

Indeed, the majority of videos digitally forged that are currently circulating online contain sexual images of women. Deepfake technology has made it relatively easy to 'undress' someone or swap their face into an already existing pornographic video. **It has been estimated that between 90% and 95% of all digital 'deepfakes' concern** material depicting nudity or sexually explicit activities.[52] **The vast majority of those 'deepfakes' (90%) concern women**. In 2020, a Telegram chat bot that can be used to create deep nude portraits was created. By providing the chatbot a picture of someone, one could receive an undressed version of this person. The bot exclusively created nudes of women. By the time of the public report, already over 100,000 women were targeted.[53]

Moreover, according to a report by EPRS, **sexual digital forgeries**[54] **can be used to discredit female journalists and politicians** posing a threat to democracy. Digital sexual forgeries exacerbate existing gender inequalities and power relations. Forcing women into a virtual sexual context, reduces them to defenceless objects.[55] Because they are so realistic, digital forgeries can misrepresent reality. By exploiting people's inclination to trust the reliability of evidence that they see with their own eyes, digital forgeries can turn fiction into apparent fact.[56]

The gender aspect of digital forgeries has also been highlighted by other studies. According to the 2023 report by Equality Now, **women and girls particularly face amplified risks and unique challenges in combatting deepfake image-based sexual abuse**.[57] In line with this, the Cyber Rights Organisation found that 90% of victims of the distribution of non-consensual intimate imagery, including sexual digital forgeries, are women, who are disproportionately targeted and threatened by male perpetrators in different spaces of the web.[58]

Moreover, **young people seem particularly affected by sexual digital forgeries ('deepfakes')**. A 2024 survey examines the prevalence of deepfakes among Belgian people aged 15-25 years (N=2819). It found that 41.9% of respondents had heard the phenomenon. In addition, 23.1% of respondents had seen a 'deepfake' image, mainly in Snapchat, Twitter and Instagram. Among those who were aware of 'deepfake' apps (12.8%) 60.5% tried to create them. The motivations ranged from revenge to a desire to impress friends.[59]

Virtual reality and the metaverse

3D technology, virtual reality and the metaverse have also created new digital spaces for misogyny and online abuses against women. [60]

3D animation technology is increasingly able to generate videos with a similar quality to AI-based deepfake.[61] Some 'deepfake' programmes even combine AI image generation and 3D animation. Most notably are **avatar technologies** that animate 3D models of a person's head or entire body. 3D facial animation techniques were used in cinema movies and computer games; however, in the past five years, the popularity of **virtual reality and augmented reality**[62] **technology** has increased, due to the availability of equipment at a consumer-friendly price. Large

Immersive and haptic technologies make the experiences of sexual assault in the metaverse as intense and traumatising as offline abuses

technology companies, such as Facebook, are also investing in technological developments, such as the **Facebook Codec Avatar**.

The use of 3D avatars has spread also in the metaverse. As **Meta** expands access to its virtual reality platform, the **number of disturbing accounts of women being sexually assaulted and harassed has increased**. Women have reported experiencing their avatar being cornered or trapped in a virtual room, by one or numerous assailants, who performed other violent or sexual assault behaviours against the avatar. Incidents include attacks to the vice-president of a metaverse company who claims that she was groped by a group of male avatars within 60 seconds after joining, as well as the sexual assault to a researcher who had joined the virtual reality platform to study users' behaviour and was assaulted within one hour. [63]

Immersive and haptic technologies make the experiences of sexual assault in the metaverse as intense and traumatising as offline abuses. Victims describe their virtual experiences as real. The panoramic view, audio and the touch simulation provided by the virtual reality headsets and handheld controls create a multi-sensory experience, blurring the separation between the virtual and the physical. The **continuum of violence must also be considered**, giving the connections and continuities between different forms of violence be it online or offline, virtual or physical. As pointed out by various academics, gamers experience visceral responses to online assaults in their physical real body[64] [65] and may experience re-traumatization of previous sexual assault or abuse they had in the physical world. As Weiderhold states: 'If you've had this [sexual violence] happen to you in the metaverse, it doesn't end when you take off the headset'.[66]

Online Gaming

As more women join **online gaming communities**, they report experiencing high rates of sexual harassment online. VAW in the context of online games has been explored in the literature. Jenson and De Castell[67] describe the gaming realm as one composed of 'particularly hostile environments to those identifying or identified as women'. A 2021 qualitative study[68] shows that there are mainly two types of VAW present in the online gaming communities: psychological and sexual harassment. The spread of psychological violence is directly linked to gender stereotypes, based on curses. The sexual harassment occurred with the persistence of objectifying the female body in games, causing embarrassment to the players. Moreover, four studies explored

the prevalence of sexual harms in online gaming environments (sample sizes ranged from 127 to 1,682). Rates of online sexual harassment ranged from 34.2% to 84.3%, with one study showing women received 11 times more sexual harassment comments than their male gaming counterparts.[69]

Academics agree on the fact that online gaming communities are perceived as one of the **most inequitable online environments for women**.[70] [71] For example, in 2019, a developer (Desk Plant) released Rape Day, a game centred on a serial killer and rapist who, during a zombie apocalypse, rapes and kills women. The game was cancelled before being publicly released.[72] This inequity is rooted in the construction of the gamer identity around the male identity.[73] Online video gaming communities have normalized the oppressive structures and phenomena of traditional patriarchal societies.[74] These include the sexually objectified, powerless, and disproportionately small representations of women within games and gaming communities, as well as the perpetration and legitimization of online and offline aggression towards female gamers. [75]

This is partly due to the fact that the gaming realm is characterized by the dominance of male programmers, developers, marketers, and manufacturers who have persisted in advancing sexualisation of gaming avatars and characters and embedded sexualisation and sexual violence within their gaming scenarios and rewards.[76]

3.3 MACRO-FORMS

While the forms of CVAW are numerous and are defined differently across countries and stakeholders, some **macro-categories** of CVAW can be identified. These categories are those on which the majority of Member States have adopted legal and policy instruments; they correspond to the main forms of CV covered by the Directive on VAW (see section 3.2).

As mentioned in Section 2.1, the macro-forms of CVAW outlined below should not be regarded in isolation but as interlinked with offline violence. **Digital tools can exacerbate violence occurring offline**. For example, some forms of VAWG such as intimate partner, domestic violence and trafficking in human beings are facilitated through different digital tools including mobile phones, GPS and tracking devices amongst others. Abusive partners and/or ex-partners use tracking devices or other digital tools to monitor, track, threaten and perpetrate violence.[77] Traffickers in human beings use technology to profile, recruit, control and exploit their victims.[78]

The macro-forms of CVAW are identified as:

- **Cyber stalking against women**: Article 34 of the Istanbul Convention[79] defines stalking as 'intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety'. The Explanatory Report[80] further acknowledges that stalking committed via the use of ICT is covered by Article 34. The threatening behaviour may consist of repeatedly following another person, engaging in unwanted communication with another person or letting another person

know that he or she is being observed. Engaging in unwanted communication entails the pursuit of any active contact with the victim through any available means of communication, including modern communication tools and ICT devices.

Stalking practices committed in the digital sphere include threats, damage to reputation, monitoring and gathering of private information on the victim, identity theft, solicitation for sex, impersonating the victim and harassing with accomplices to isolate the victim. It usually involves the tactic of surveilling or spying on the victim, on their various social media or messaging platforms, their e-mails and phone, stealing passwords, cracking, or hacking their devices to access their private spaces, via the installation of spyware or geo-localisation apps, or via stealing their devices. Perpetrators can also take on the identity of the other person or monitor the victim via technology devices connected through the Internet of Things (IoT), such as smart home appliances.

Research shows that cyber stalking has a gender dimension. According to the 2014 FRA survey, 5% of EU women have experienced cyber stalking since the age of 15.[81] At global level, 63% of women have experienced cyber stalking according to the 2021 Report by the Economist Intelligence Unit.[82]

- **Cyber harassment against women**: Cyber harassment is the persistent and repeated unwanted course of conduct, targeted at a specific person, designed to cause severe emotional distress and often a fear of physical harm.[83] Cyber harassment can take many forms including: unwanted sexually explicit emails or text (or online) messages; inappropriate or offensive advances on social networking websites or internet chat rooms; threats of physical and/or sexual violence by email or text (or online) message, etc.[84] Online harassment can be perpetrated by a single individual or a group of individuals, usually networks of male perpetrators who target women and minorities.

Evidence shows that women and girls are particularly vulnerable to cyber harassment. The 2014 survey by FRA[85] highlights that 11 % of women and girls had experienced cyber harassment since the age of 15 across the EU. According to the 2019 FRA's survey, 13 % of women had experienced cyber harassment during the previous 5 years.[86]

- **Non-consensual intimate image abuse (including sexual digital forgeries, commonly known as 'deepfakes')**: intimate image abuse consists of the non-consensual creation, manipulation and dissemination, mostly online, of intimate or private images/videos or images/videos of a sexual nature or threats to do so.[87] These images/videos may have been obtained with or without the consent of the person pictured in the image.

Some academics prefer to use the wording 'image-based sexual abuse', which include a broader spectrum of abuses than the term 'non-consensual intimate image abuse'. According to Clare McGlynn,[88] image-based sexual abuse refers to the taking or sharing of nude or sexual photographs or videos of another person without their consent. It includes a variety of behaviours such as those listed in the table below - non exhaustive list.

As highlighted by McGlynn, image-based sexual abuse accurately conveys the significant harms that may occur and reflects the experiences of victim-survivors. It also identifies image-based sexual abuse as a form of sexual violence, locating it within sexual offence law and policies.[89]

Forms of image-based sexual abuse (IBSA)	
Sextortion	Sexual extortion, also called 'sextortion', is the act of using the threat of publishing sexual content (images, videos, digital sexual forgeries, sexual rumours) to menace, coerce or blackmail someone, either for more sexual content or for money, sometimes both.
(Abusive) Sexting	Abusive sexting is the non-consensual electronic sharing of naked or sexual photographs.
Filmed assault	Filmed assault, also known as 'happy slapping', is the act of attacking (physical attack or sexual assault) a victim with the objective of recording the assault and sharing it online. It can be included in the macro category of image based sexual abuse.
Upskirting creepshots and digital voyeurism	Upskirting, creepshots and digital voyeurism. These forms of IBSA and sexual surveillance involve taking non-consensual photos or videos of survivors, mainly women and girls, in public places such as stores, public bathrooms, locker rooms, classrooms or the street; but also in their own apartments. They may entail taking images up a person's dress or skirt (upskirting, taking a sexually suggestive picture of a woman without her noticing (creepshot) or surveilling or surreptitiously observing with the use of technological tools, and in some cases recording, another person in what would generally be regarded as a private place (digital voyeurism).

Image-based sexual abuse is also known as 'revenge pornography' or 'non-consensual pornography' in the national laws of some Member States. However, the term should be avoided according to experts in the field, as it minimizes the impact of this crime on people's lives. The term 'pornography' does not denote the non-consensual nature of the act, and the term 'revenge' only focuses on the presumed motive of the perpetrator, excluding the experience and rights of the victim. Moreover, many perpetrators are not motivated by revenge or by any personal feelings towards the victim. Image-based sexual abuse is a gendered harm, with perpetrators being mostly men, women particularly victimised, and the harms made worse by sexual inequalities.[90] The use or dissemination of intimate or private images is highly gendered; studies and data show that women and girls are the main targets of digital sexualised violence and that they are disproportionately affected by it (Uhl et al., 2018; Henry and Flynn, 2019; Dunn, 2020; Henry et al., 2020).[91] According to the results of a 2019 study that examined the rates of image-based sexual abuse victimisation and perpetration in the US, women face significantly higher rates of victimisation and significantly lower rates of perpetration than men (Ruvalcaba and Eaton, 2019).[92]

- **Online gender hate speech**: Online hate speech is an umbrella-term covering all forms of expression, which share, encourage, promote or justify race hatred, xenophobia, anti-Semitism or every other form of hatred based on intolerance including aggressive nationalism, ethnocentrism, discrimination and hostility of minorities, emigrants or persons of foreign origin.[93]

As noted by EIGE, online gender-based hate speech tends to target women and girls in all their diversity because of their gender.[94] It can take many different forms such as: sexualisation, objectification, body shaming or cruel remarks regarding their gender, but also their religion, ethnicity, disability or sexual orientation. Female journalists, politicians, activists and other public figures are particularly vulnerable to hate speech. Women who express their opinions online are subject to heavy repercussions (see Section 2.8).

3.4 ADDITIONAL FORMS

In addition to the macro-forms of CVAW, there are many additional **forms of CVAW**. Overlaps may occur between the various forms (e.g. 'digital dating abuse' may intersect with 'non-consensual sharing of intimate images'). It also should be noted that some manifestations of CV may be considered as 'tactics used by perpetrators' rather than forms (e.g. non-consensual sharing of images may be classified as a tactic to commit 'cyber harassment').

The table below provides a description of some additional forms of CV. However, these phenomena are in continuous development and, thus, **definitions continue to evolve**. The list is non-exhaustive given that new forms continue to emerge with the increase in digitalization and the rapid evolution of technology.

Form of CV	Description
Astroturfing	Dissemination or amplification of content (including abuse) that appears to arise organically at the grass-roots level and spread, but is actually coordinated (often using multiple fake accounts) by an individual, interest group, political party or organization.
Body shaming	Body shaming consists of commenting on and mocking someone's bodily shape, size or appearance. It may be categorised as cyber harassment or online hate speech.
Catfishing	Internet scam where the abuser pretends to be someone they are not, by creating false online identities in social media – often using other people's photos and developing extensive fake life stories and experiences, jobs and friends – with the objective of seducing another person or making them believe they are in an online relationship and use this as a means to ask for money, gifts or intimate images.
Cyber bullying	Cyber bullying is an umbrella term that refers to a wilful and repeated harm inflicted through the use of computers, cell phones and other electronic devices, with the aim of frightening and undermining someone's self-esteem or reputation. This term is mainly used in relation to children and young people.
Cyber flashing	Cyberflashing consists of sending unsolicited sexual images using dating apps, message apps or texts, or using Airdrop or Bluetooth. Most often, cyberflashing occurs when someone sends an unwanted picture of genitals or exposes himself/herself over live video. Cyber flashing can be done by someone you know or by a stranger. It can happen in lots of different situations - for example: on dating apps or websites; on social media; over text, WhatsApp, or other messaging apps; during a video call; over email; or through Airdrop or another app that allows someone to share files with people close by. Cyber flashing can be considered a form of online harassment.
Cyber mobbing or mobbing	Cyber-mobbing (or mobbing, dogpiling, networked harassment) consists of organized, coordinated and systematic attacks by a group of people against particular individuals or issues, such as by groups that target feminists or people who post about racial equality issues online.

Digital dating abuse	'Digital dating abuse' involves using technology to repetitively harass a romantic partner with the intent to control, coerce, intimidate, annoy or threaten them. It includes the following behaviours: looking through the contents of the partner's device without permission; keeping the partner from using their device; threatening the partner via text; posting something publicly online to make fun of, threaten, or embarrass him/her; or, posting or sharing a private picture of the partner without permission. It includes digital romance/love scams.
Doxing	Doxing is the act of sharing online a target's personal information (phone number, e-mail address, home address, professional contacts) without consent, to encourage abuse.
Flaming	Flaming is the act of posting offensive or hostile messages, including insults, on social networks or forums.
Google bombing	The terms Google bombing and Google washing refer to the practice of causing a website to rank highly in web search engine results for irrelevant, unrelated or off-topic search terms by linking heavily. It works by creating a large number of backlinks, typically using exact-match anchor text, to a particular webpage, which makes it rank high for a specific, often unrelated query.
Malicious distribution	Malicious distribution is the use of tech tools to distribute defamatory material related to the victim and/or organizations; e.g. by using new technologies as a propaganda tool to promote VAW, call for violence against abortion providers, etc.
Hacking	Use of technology to gain illegal or unauthorized access to systems or resources for the purpose of attacking, harming or incriminating another person or organization by stealing their data, acquiring personal information, altering or modifying information, violating their privacy or infecting their devices with viruses.
Identity theft or online impersonation	From a legal perspective, the Organisation for Economic Co-operation and Development (OECD) describes 'identity theft' as a crime occurring 'when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes'. From a criminological perspective, three stages of online identity theft and related crimes can be described: obtaining or 'stealing' the identity data, trading in stolen identity data and the abuse or (mis)using the data for a criminal purpose. The criminal use, in turn, can be for financial (e.g. fraud) or non-financial (e.g. libel) purposes. Identity theft can take many different manifestations such as catfishing (see above).

Online child sexual assault (also known as grooming)	Specific type of technology-facilitated sexual experience by which children and young people are contacted through social media or other digital platforms with the purpose of sexually assaulting them. Online child sexual assault consists of setting up an online abusive relationship with a child, in order to bring the child into sexual abuse or child-trafficking situations.
Sealioning	Rhetorically, sealioning fuses persistent questioning—often about basic information, information easily found elsewhere, or unrelated or tangential points—with a loudly-insisted-upon commitment to reasonable debate. It disguises itself as a sincere attempt to learn and communicate. Sealioning thus works both to exhaust a target's patience, attention, and communicative effort, and to portray the target as unreasonable. While the questions of the 'sea lion' may seem innocent, they are intended maliciously and have harmful consequences.
Zoom bombing	Zoombombing is a type of cyber-harassment in which an unwanted and uninvited user or group of such users interrupts online meetings on the Zoom video conference app. This disruption occurs when intruders gate-crash digital gatherings - sometimes for malicious purposes, such as sharing sexually explicit or hate images or shouting offensive language - without the host's permission.
Trolling	Trolling is deliberately posting abusive comments online, sometimes with the express intention of causing alarm, distress or humiliation. The attacks can also be carried out by a group of people in a co-ordinated and targeted manner.

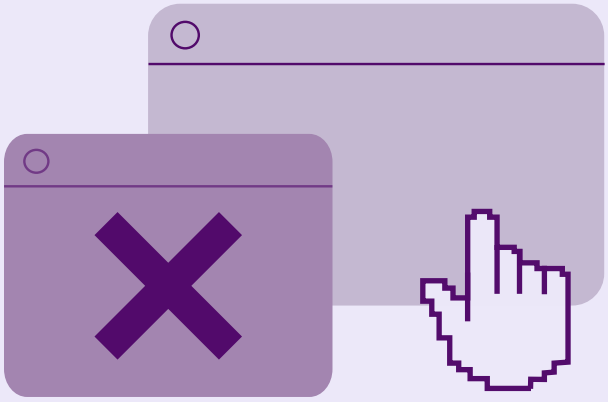
The Manosphere

The manosphere is a network of online men's communities advocating for various men's rights and interests, while promoting misogynistic ideologies, anti-feminist and sexist beliefs. They blame women and feminists for all sorts of problems in society. Many of these communities encourage resentment, or even hatred, towards women and girls.[95]

Key segments include: Men's Rights Activists (MRAs), who claim to focus on issues affecting men often opposing feminist movements; Pick Up Artists (PUAs)[96] who emphasise men masculinity vis-à-vis women weakness and promote a game of seduction based on power unbalance; Incels (Involuntary Celibates)[97], who express resentment towards women due to their perceived sexual rejection; and Men Going Their Own Way (MGTOW), who advocate for complete disengagement from women. These groups have leveraged social media and online forums to propagate their views, influencing public discourse and policy debates.

They often perpetuate harmful stereotypes and foster environments that can incite real-world VAW. Understanding and addressing the impact of these online hate communities is crucial for promoting a more inclusive and equitable society.

This form of CV can overlap with the macro-category of gender hate speech.



Pornography

Pornography is a form of sexual violence against women with an online and offline dimension. Pornography is not only based on the objectification of women's bodies promoting damaging stereotypes in its portrayal of women; but it also entails acts of sexual violence with the intent of normalising them as sex. The production of pornography entails sexual violence against the women and girls being filmed and it is linked to the system of prostitution. It also encourages VAW as it plays a key role in shaping men's and women's conceptions of relationships. Pornography has a strong influence on both beliefs and behaviours; it can lead not only to specific sexual scripts, but it can affect also general attitudes toward women and children, to what relationships are like, and the nature of sexuality. Besides, pornography normalises violence and makes violence sexy.[98] Figures show that the states with higher circulation rates of pornographic magazines have higher rape rates.[99]

The degrading way in which women are portrayed in pornography has an impact on all women and increases men's VAW. Studies have shown that high percentages of female victims of domestic violence or women in prostitution victims of sexual abuse report that their abuser were viewers of pornography.[100]

The rapid growth of pornographic sites on the internet facilitates men's and boys easy access to pornography making this form of GBV accessible every minute of the day in both the public and the private spheres of women and men's lives.

According to the EWL, pornography should be considered an element of the system of prostitution and thus as forming a part of the continuum of male violence against women and girls. Actual exploitation of women and girls is found on pornographic websites, publicly broadcasting sexual assaults, rapes and acts of torture. It is often used as a means of grooming women for traditional prostitution and victims of sex trafficking are often filmed. Various testimonies coming from women previously exploited in this 'industry' confirm that they were very often coerced to do practices at the last moment, while the camera was already shooting

and when the producers would not allow them to stop.[101]

Women in pornography have also been denouncing the frequent use of drugs or alcohol that is encouraged to overcome the trauma caused by the scenes they had to shoot and the times they were blackmailed to not be paid if they refused an act. Extremely affected physically, these women and girls are also more prone to experience mental issues than the rest of the population. Lately, an increase of suicides was observed among women exploited in the pornographic field. According to the EWL, this is especially worrying since young people tend to use pornography as a form of sexual education, particularly when comprehensive sexual education is not provided in their country and/or when sexuality cannot be discussed at home, meaning that they are more likely to reproduce these kinds of abusive and discriminating behaviours during their own sexual encounters.[102]

4. HOW PREVALENT IS CYBER VIOLENCE AGAINST WOMEN?

The **lack of agreed definitions** of CV (see Section 2.2) **and methodologies for its measurement make it particularly difficult to assess the extent of the problem**.[103] Many countries collecting data through prevalence surveys on VAW, do not include questions on CV. The countries that have dedicated surveys use different definitions and methodologies, making the available data not comparable. **This lack of comparable data, in addition to under-reporting, contributes to the under-estimation of the actual prevalence rates of CVAW**. Only 1 in 4 women globally report incidents of CVAW to the online platform(s) on which it occurred.[104]

Despite these gaps and differences in methodologies, **some attempts to measure CV have been made at both international and EU level**. While these attempts do not provide a holistic picture of CVAW, they should be considered as important efforts to give an overview of the phenomenon.

At **international level**, a global report[105] which synthesized results from surveys on online VAWG, from 2018 onwards, estimated that between 16-58 % of women have experienced TF VAW. Similarly, the Economist Intelligence Unit found that 38% of women have had personal experiences of online violence, and 85% of women who spend time online have witnessed digital violence against other women.[106] Moreover, nearly three-quarters of surveyed women expressed concern about online abuse escalating to offline threats, showing the interconnections between online and offline violence (see section 2.1). A 2021 survey of 51 countries, including many European countries, reported that 57% of women had been victims of image-based sexual abuse.[107]

The phenomenon does not concern a specific region but equally affects all geographical areas of the globe. Moreover, women in countries with long-standing or institutionalized gender inequality tend to

experience online violence at higher rates.[108] Likewise, a 2017 survey of women aged 18-55 and covering eight countries (Denmark, Italy, New Zealand, Poland, Spain, Sweden, the UK and the USA) found that 23 % of women reported at least one experience of online abuse or harassment. A 2023 survey conducted by UN Women[109] in Eastern European Countries and Central Asia indicates that more than half of adult women in the region (53.2%) have experienced some form of TFV against women at least once in their lifetime.[110]

CVAW seems to increase in crisis situations. During the COVID-19 pandemic, a peak in digital violence occurred. In Australia, there was a 210% increase in image-based abuse linked to the pandemic. Data from India, Sri Lanka, and Malaysia showed a 168 % increase in the volume of misogynistic online posts during the lockdowns.[111] The World Wide Web Foundation's report of 2020 covering 180 countries found that during the pandemic, 52% of young women and girls had experienced online abuse, including threatening messages, sexual harassment and the sharing of private images without consent.[112]

The severe lack of data and research on CVAW is a major issue also at EU level. Due to this, an adequate assessment of the prevalence and impact of CVAW is not possible. According to EIGE, a holistic and up-to-date estimate of the prevalence of CVAW is missing. Most Member States do not collect data on CVAW consistently and, where data is available, the scope is rather generic, or limited to specific forms of CV.[113]

Some attempts to measure the prevalence of some forms of CVAW at EU level have been made by the FRA back in 2014 and 2019.[114] The 2019 FRA's survey collected data through self-reporting from around 35,000 people across the EU, the UK and North Macedonia.[115] The survey found that 13% of women had been subject to cyber-harassment in the five years before.

Other interesting data come from the 2021 survey by HateAid.[116] The survey asked 2,000 people between the ages of 18 and 80 from all EU countries about their experiences with digital violence. The results indicate that: 50% of young adults in the EU are affected by hate on the internet; 30% of women across the EU fear that fake intimate images of them may be shared without their consent; 80% of respondents give online platforms a poor report card.[117]

At **national level**, although some EU Member States collect data on CV (mainly through surveys rather than administrative data) this data presents several limitations:[118] it is often mixed with data on offline violence; it covers only specific forms of CVAW; it mixes together different forms of CVAW; it covers different age groups; it is based on different definitions and methodologies that make it not possible to compare data.

To provide some examples, across Germany, France, and Spain more than one in two (53%) of women aged 18-34 have been a victim of image-based abuse. Of women victimised, 82% reported feeling less safe, with some looking to withdraw entirely from online spaces.[119] In France, more than 4 out of 10 people say that they have been victims of cyber harassment.[120]

5. WHERE DOES CYBER VIOLENCE AGAINST WOMEN TAKE PLACE?

According to a UN Women's review[121] of studies that compare different contexts of TF VAW, women are more likely to experience violence on **social networking sites**, compared to other digital contexts. While several social media platforms are mentioned (including Twitter, WhatsApp, Instagram and Reddit), Facebook seems to be the most common site for online gender-based violence. However, this might be due to Facebook's popularity compared to other social media platforms. Similar findings come from a 2023 UN Women's study[122] covering Eastern European countries and Central Asia.

Facebook, Instagram, TikTok, E-mail or messaging applications (Skype, Snapchat, messenger, Viber, etc.), WhatsApp, Telegram, YouTube are the platforms where women have experienced CVAW.

Differences among social platforms can be noted according to the form of CV. For example, cyberbullying occurs mostly on YouTube, TikTok, Snapchat and Facebook.[123] A French survey by IPSOS[124] indicates that cyber harassment is widespread on Whatsapp, Instagram, Facebook and Twitter, Discord and Snapchat. A study by Amnesty International[125] found that for many women X (previously Twitter) is a platform where CVAW flourishes. Incidents of CVAW on Twitter include: direct or indirect threats of physical or sexual violence, discriminatory abuse targeting one or more aspects of a woman's identity, targeted harassment, and privacy violations such as doxing or sharing sexual or intimate images of a woman without her consent.

While research indicates that social networks as the most common spaces for CVAW, it should be noted that networking sites are the most commonly studied context of TF VAW,[126] followed by communication technologies and personal online accounts. **Few studies investigate**

Other spaces for the proliferation of CVAW are the pornography platforms that embody the sexual objectification of women and girls and promote sexist and violent power-relations.

violence on dating or entertainment sites, as well as GPS-based and 'smart home' technologies.[127]

Moreover, evidence shows there are certain **differences between perpetrators related to types of platforms** they use to commit CVAW: partners more often use Twitter, WhatsApp, and meeting tools; friends and acquaintances more often use Telegram, TikTok, and online gaming platforms; while persons only known to women online tend to prefer Facebook, Instagram and dating platforms.[128] Nonetheless, it should also be taken into account that **CVAW can start in one platform and spread in others**. According to an Indian study, CVAW can jump from one platform to another. Women subject to online harassment reported that men who are rejected on dating platforms harass women with repeated 'friend requests' on platforms such as Facebook.[129]

Other spaces for the proliferation of CVAW are the pornography platforms that embody the sexual objectification of women and girls and promote sexist and violent power-relations.[130] Despite the large pornography platforms stating they have policies against non-consensual material on their websites, such material is easily and freely available. There are many types of CVAW on porn websites specific to image-based sexual abuse, including upskirting, spycams, hidden cams, leaked and stolen sexual images.[131]

The largest study to date of online porn content indicates that 1 in 8 titles on the front page of the most popular pornography websites describe sexually violent material, including image-based sexual abuse, with voyeurism images as the most common.[132] According to experts, porn companies are actively choosing to showcase this material to new users, demonstrating that their business model promotes illegal and harmful content.[133] In this regard, McGlynn and Woods offer new and compelling evidence that the boundary between what is and is not sexual violence is distorted by mainstream online pornography platforms.[134]

6. WHO ARE THE VICTIMS OF CYBER VIOLENCE?

Cyber violence has a gender dimension. As mentioned in Section 2.1, while men can also be victims of cyber violence, women and girls are more likely to experience unique forms of gendered violence in digital contexts. This points to a similar pattern to offline violence.[135]

According to a 2023 FRA's report focusing on online hate in social media posts, **women face more harassment than any other target groups based on their ethnic origin** (people of African descent, Jews and Roma).[136] **Misogyny is the most prevalent form of online hate** across all the examined platforms. For example, the number of posts targeted at women is almost three times that of those targeted at people of African descent across the four countries covered. Posts targeted at women most often include denigrating language. There are also **higher levels of incitement to violence against women compared to the other groups**, with cyber violence against women most often based on **sexualised violence**. Women are also particularly **targets of harassment**: two-thirds (67 %) of all hateful posts targeted at women were found to be harassment.

Similarly, an American study found that 33% of women under 35 report having been sexually harassed online, compared to 11% of men. Out of the total female victims, 47% think they have encountered harassment because of their gender, whereas 18% of men who have been harassed online believe the same.[138]

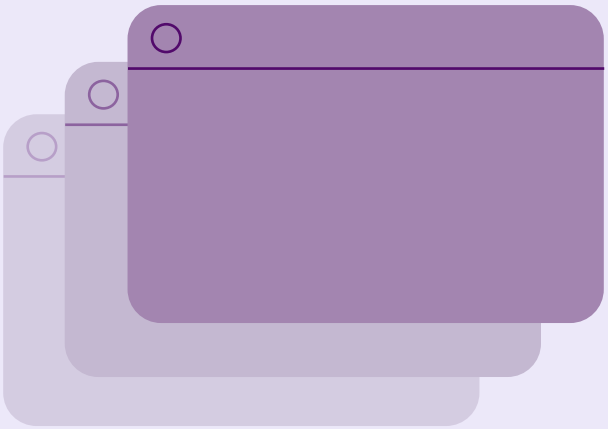
Along the same lines, GREVIO highlights that both men and women may experience incidents of inter-personal violence, however, **women are considerably more likely to be subject to repeated and severe forms** of abuse, both offline and online. Already in 2018, the UN Special Rapporteur on VAW had warned that the Internet is used in a broader environment of widespread and systemic structural discrimination and GBV against women and girls. Emerging forms of ICT facilitate new types of VAW.[139] **The consequences of and harm caused by different manifestations of CV are specifically gendered**, given that women and girls suffer from particular stigma in the context of structural inequality, discrimination and patriarchy. **Women subjected to CV are often further victimised through harmful and negative gender stereotypes** (see section 2.8).

Moreover, while all women that have access to digital spaces are exposed to risks of CV, evidence highlights that **some groups of women are particularly vulnerable**. According to GREVIO, digital forms of gender-based VAW can be particularly pronounced for women and girls at risk of or exposed to **intersecting forms**

of discrimination, and may be exacerbated by factors such as **disability, sexual orientation, political affiliation, religion, social origin, migration status or celebrity status**, among others. Likewise, a 2023 report by the Global Partnership shows that women who experience intersecting inequalities are disproportionately impacted by CVAW. [140]

With regards to women with disabilities, a study shows that women with **intellectual or cognitive disability** can be particularly susceptible to CV.[141] In 2022, according to a report by Vox, the Italian Observatory on Rights, which monitors hate expressed on social media via Twitter, women were the most affected followed by people with disabilities.[142] Similarly, Amnesty International found that women with disabilities, among other groups, experience higher rates of online abuse on Twitter.[143] For example, an Irish Politician from Belfast told Amnesty International that the abuse she has received on social media platforms not only focuses on her appearance but also targets the fact that she has a disability. She stated: '*I have a physical disability and that has often been commented on – about how I should 'get that disability fixed*'. Recently women with disabilities have been insulted and offended by a youtuber, who, in a 90-minute broadcast and 50,000 views, using sexist and macho language described his sexual fantasies with girls with disabilities, especially with Down syndrome, denigrating them and reducing them to passive sexual objects.[144]

Moreover, CV can be stronger towards women from racial minority groups and different religious communities.[145] For example, women of colour are more impacted by violence online or through digital means than white women, with Black women being 84% more likely to receive abusive tweets on Twitter.[146] Women belonging to religious or ethnic minorities may also be a particular target. Among migrants, second generations and minorities, physical and online harassment can lead to lower trust in institutions and ultimately damage social integration.[147]



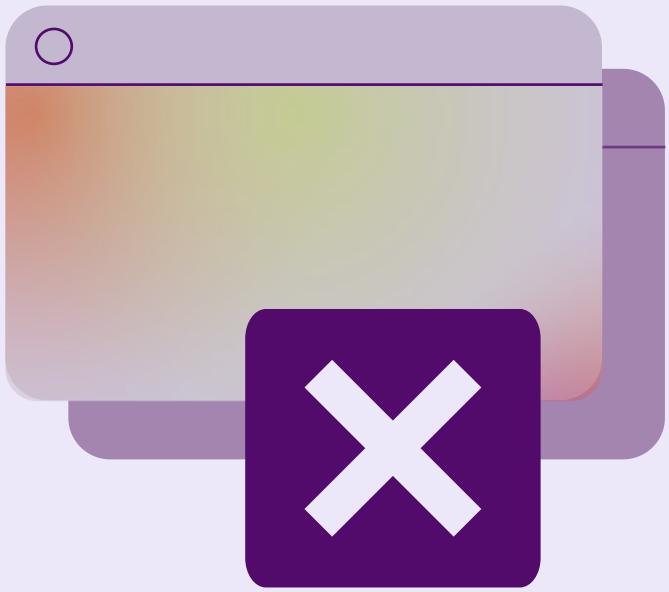
Women in public life including women's rights activists, women human rights defenders, women in politics, and women journalists are also often targets of CV. According to a study by UNESCO, 73% of women journalists have experienced online violence in the course of their work, including threats of physical and sexual violence, along with digital security attacks.[148] A 2021 study of women in parliaments in Africa highlights that 46% of women parliamentarians had been subject to sexist attacks online.[149] In 2023, the Council of European Municipalities and

Most girls report their first experience of social media harassment between the ages of 14 and 16.

Regions (CEMR) conducted a Europe-wide survey on VAW in politics among locally elected female politicians; 2 242 politicians in 31 European countries shared their experiences of violence. According to the results, 32 % of respondents had experienced violence; the vast majority of cases consisted of cyber violence (48%).[150] Women who are politically active online tend to be subject to insults, hate speech, reputational risk, physical threats and sexualised misrepresentation (see Section 2.8).[151] Women activists are targeted with forms of abuse intended to silence them, including, 'pile-ons' where activists are targeted by coordinated waves of different forms of online abuse.[152] Furthermore, women who advocate, especially in the area of gender justice, experience higher rates and more severe online violence than other women.[153]

Women of all ages are vulnerable to CV; however, the intersection of age and gender discrimination, alongside the higher level of ICT use amongst **young women**, increases their vulnerability to online violence. Research indicates that young women and girls are particularly exposed to online violence. One study[154] found that 58% of girls and young women surveyed globally have experienced some form of online harassment. Most girls report their first experience of social media harassment between the ages of 14 and 16.

Specific age trends according to the form of CV are noted by EIGE. While girls and young women are more vulnerable to certain forms of CV (e.g. cyber bullying and non-consensual intimate image abuse), older women tend to be exposed to other forms (e.g. identity theft and cyber harassment).[155] The tendency of young people to overlook safety issues and take more risks as well as the poor digital skills of older victims are some of the reasons behind this trend.



7. WHO ARE THE PERPETRATORS OF CYBER VIOLENCE?

CVAW can be perpetrated by both men and women. However, in the majority of cases women tend to be targeted by men, who can be unknown or known to the victim.[156]

For example, the vast majority of perpetrators of image-based sexual abuse are men.[157] Although the motivations of perpetrators vary, a dominant theme is that of power and control. A 'collector culture' is also flourishing among men, where men are trading and sharing intimate images without consent across internet fora and private groups.[158]

As explained in Section 2.1, technology has also provided opportunities for CVAW to be committed **anonymously** with relative impunity. A study by Plan International across 31 countries found that **strangers are the most common perpetrators of CV** against young women and girls (36%), followed by anonymous social media users (32%) and acquaintances on social media (29%). Moreover, 16% of online abuse against young women and girls is perpetrated by groups of strangers.[159] Among older women, 59% of women subject to abuse or harassment on Twitter said they were attacked by strangers.[160]

However, **perpetrators of CVAW can also be known to the victim**. Perpetrators include current and former intimate partners who misuse and abuse technologies to control, harass, intimidate and monitor the movements of victims-survivors.[161] This finding confirms the **continuum of violence** between the offline and virtual world (see section 2.1). In this regard, an Australian study found that former intimate

partners, current intimate partners and date, short-term or casual sexual acquaintances were the most common perpetrators of CVAW.[162] In the context of intimate partner violence (IPV), technology is often used to intimidate, coerce and maintain control over the victims in order to maintain a relationship or as a punishment or revenge for having left them, as well as a platform to incite others to harm them or to interfere with legal proceedings, among other reasons.[163]

Abusive intimate partners stalk, monitor and threaten their victims through location-based services, social media and spyware that is readily available on official app stores, some of which is even advertised to abusers as tools to 'Catching Cheating Spouses'.[164] Perpetrators often have access to their (ex)partner's accounts, thereby easily gaining illicit access to survivors' devices and accounts, including email and social media accounts, and banking information.

Having access to these private data may allow perpetrators to install spyware, to track and monitor survivors' location and technology use, to steal or delete survivors' information and to impersonate the victim.[165]

Perpetrators can be one or a multitude. A study in Africa notes that in 57% of cases one specific person was the perpetrator and in 23% of cases multiple perpetrators were involved with evidence of an increase in organised attacks, especially against women with public-facing careers including journalists, activists and politicians.[166]

As stressed by the UN Expert Group, it is also important that different categories of perpetrators are captured by research. Given the fact that technology allows the easy and fast dissemination of content harmful to women, both **primary and secondary perpetrators** should be identified. For example, one person may share a non-consensual intimate image (primary perpetrator) which may then be viewed and shared by a multitude of users (secondary perpetrators).[167]

8. WHAT ARE THE MAIN IMPACTS OF CYBER VIOLENCE ON WOMEN?

As highlighted by UNFPA, TFGBV is often perceived as a less serious and less harmful form of GBV; nonetheless, it can have as serious consequences on the health and lives of women as physical and sexual violence.

The **public, pervasive, repetitive and perpetual nature of TFGBV as well as the interconnections between online and offline violence, make survivors feel in constant fear and insecurity**.[168] As explained in Section 2.1, the violent content spread online, including image abuse, becomes persistent, difficult to remove and, therefore, re-traumatizing for the victims.

GREVIO refers to **severe psychological, economic and social impacts of CVAW**. As for psychological impacts, abusers can misuse technology to track the whereabouts of their victims; such forms of violence have a devastating mental toll on women. Moreover, in digital forums, economic abuse can manifest itself as controlling the bank accounts and financial activities of the victim through internet banking, using credit cards without permission or filing all financial contracts in the name of the victim. Digital violence can also lead to social consequences such as women's self-censorship and digital exclusion.

Likewise, the EPRS's report[169] emphasizes the **deep and pervasive consequences of CVAW**. These include: reputational damage, mental illness, disruptions to living situations, invasions of privacy, silencing or withdrawal from the online environment, and damage to personal relationships and reduced engagement in democratic life. In addition to effects at the individual and social level, there are also **significant financial consequences of CVAW** such as healthcare costs incurred as a result of harassment, damage to career prospects, job loss and time taken off work. Indirect financial effects include the costs to law enforcement agencies and victim support organisations that deal with cases of CV, as well as negative economic impacts for businesses and other organisations. The EPRS' study found that the overall costs of cyber harassment and cyber stalking to individuals and society were between €49.0 and €89.3 billion.[170] The highest costs assessed are the monetary value of the loss of quality of life and labour market impacts. Healthcare and legal costs are also substantial.

The psychological impacts of CV are particularly harmful to victims. These include severe emotional and psychological distress,

anxiety, depression, post-traumatic stress disorder and, in extreme cases, suicidal ideation, self-harm, suicide attempts[171] or suicide itself.[172] A study in eight high-income countries found out that 54 % of women who were subjected to CVAW experienced panic attacks, anxiety or stress.[173] A 2023 survey by UN Women, indicates that one in five women, subject to online violence, experienced emotional and psychological symptoms such as stress, anxiety, fear, insomnia or similar. More than one in four women felt embarrassed, one in five women felt unsafe whereas one in ten said the violence caused harm to a personal relationship.[174] In line with these findings, women victims of sexual image-based abuse describe the experience as having a devastating impact on their lives. They report having constant feelings of isolation, fear, distrust and being unsafe.[175] The impacts on the metal health are heavy and have repercussions on all aspects of women's life including education. In this regard, 18% of young women and girls who were subjected to CVAW have subsequently experienced problems at school.[176]

At **social level, the most reoccurring reactions to CVAW are withdrawal from online participation, isolation and self-censorship**. Victims of CV state that they have decreased their participation online and their engagement with technology, and they restrict or self-censor their activities in online platforms.[177] For example, the primary effect on victims of online gender-based hate speech is withdrawal from social media or other public platforms. As such, women tend to post less often, tone down their language to mitigate provocation (self-censorship) or even deactivate their accounts. Women think that by maintaining a low profile they will avoid drawing further attention to themselves. According to an Amnesty International study,[178] 76 % of women surveyed said they changed the way they used social media after experiencing cyber harassment, of which online hate speech is a form, and 32 % said they ceased posting their opinions on certain issues.

The effects on women in politics and journalism are particularly detrimental. The former tend to reduce their political activity, being dissuaded from running in elections and even leaving office prematurely. A study on women in politics notes that women who are subject to online violence tend to withdraw their candidacies.[179] Some women who are interested in politics may reconsider their ambitions when they witness disinformation campaigns against women in politics.[180] Serious impacts also affect **women journalists**. A study found that 30% of women journalists interviewed self-censored on social media as a result of online VAW.[181] Similarly, a survey of women journalists found that 37% avoided certain stories as a result of previous experience with threats, harassment or attacks.[182] The results is that CVAW limits **women's public participation and leadership; women's voices are silenced, discredited, and censored**.

Next page provides some examples of the various impacts of CV as reported by survivors.

'When the videos appeared on Pornhub it ruined my life, it killed my personality, it zapped the happiness out of me. It brought me almost two years of shame, depression, anxiety, horrifying thoughts, public embarrassment and scars. I still bear those scars. It will be an ongoing battle for the foreseeable future for myself and other survivors.'

'I felt like I did not have anyone. I tried to kill myself three times. My brother saw my videos and so did my mom.' - Mexican lived experience expert and policy advocate, Reclaim Coalition

'It (image-based abuse) is not a scandal. It is a sex crime. Just because I am a public figure, just because I'm an actress, does not mean that I asked for this.' - Jennifer Lawrence, actress and survivor of image-based abuse, The Guardian, October 7, 2014

'This not only caused isolation between my family and I, but I felt I had no one I could trust. Seven years later, I now have no contact with anyone I went to school with. I lost every friend I thought I had due to the effects of this image-based abuse.' - U.S.-based lived experience expert and advocate, Reclaim Coalition

'I divide my life into the periods before and after the stalking. It impacted whole my life. Making the case public was also traumatising.' - Victim of stalking, UN Women 2023

'I've been bullied on Twitter, by two people... I've told them to stop and to leave me alone, but they keep at it. After I told them to stop and leave me alone, I stopped communication with them but they still kept tweeting me. I feel like I can't say anything with someone on Twitter bullying me. I try to make it look like I don't care and all, but it never seems to work.' - Cyberbullying Stories - Cyberbullying Research Center

III. Legal and policy framework on cyber violence against women

This section presents an overview of the international, EU and national instruments that are directly or indirectly applicable to CVAW.

1. INTERNATIONAL

At international level, the United Nations (UN) and the Council of Europe (CoE) have addressed cyber violence. With regards to the **UN**, global processes to tackle CV have intensified during the last years, driven by the UN General Assembly, the UN Secretary General, the Special rapporteur on violence against women and Commission on the Status of Women, which have been supported by the work of UN Statistical Commission, WHO and UN Women.[183] These processes aimed to develop a common understanding of CV to enable progress regarding legal frameworks, data collection, research, statistics and other initiatives.

The table below lists in chronological order some of the main UN documents and milestones related to CV.

UN Policy documents/ milestones	Information on applicability to CV
2003 & 2011 Conclusions of the Commission on the Status of Women on gender equality in the context of technology	• 47th session (2003) related to ICT and media-based violence against women. • 55th session (2011) related to women's and girl's access to technology with a focus on education and training in the field of science and technology and their employment in these sectors.
2014 Resolution 68/181	The General Assembly expressed concerns regarding technology-related violations and abuses against women human rights defenders.
2030 Agenda for Sustainable Development (adopted in 2015)	At its heart are the 17 Sustainable Development Goals (SDGs). UN SDGs 5 and 16 refer to all forms of violence, including online. SDG 5 aims to 'eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation' (target 5.2) and 'enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women' (target 5.b). SDG 16 aims to 'significantly reduce all forms of violence and related death rates everywhere' (target 16.1).

2017 General recommendation No. 36	It focuses on the right of girls and women to education. The CEDAW Committee also recognized how girls are affected by cyberbullying, particularly in relation to their right to education.
2017 General recommendation No.35	The CEDAW Committee made clear that the CEDAW is fully applicable to technology-mediated environments.
2016 General recommendation No. 34	The CEDAW Committee highlighted the important role of ICT in transforming social and cultural stereotypes about women, as well as its potential in ensuring effectiveness and efficiency of women in their access to justice.
2018 Resolution of Human Rights Council 38/5	The Human Rights Council's resolution focuses on preventing and responding to violence against women and girls in digital contexts.
2018 Report of the Special Rapporteur on violence against women	The report addresses the causes and consequences on online violence against women and girls from a human rights perspective.
2019 Resolution of the UN General Assembly (A/ RES/74/247)	The resolution focuses on countering the use of information and communications technologies for criminal purposes.
2020 Resolution of the UN General Assembly on intensification of efforts to prevent and eliminate all forms of violence against women and girls (A/RES/75/161)	The General Assembly calls upon stakeholders to intensify their efforts at all levels to eliminate all forms of violence against women and girls and to better coordinate their work, with a view to increasing effective support for national efforts to prevent and eliminate sexual harassment.
2021 Council's Resolution on Right to privacy in the digital age (48/4)	The resolution recognizes the importance of the right to privacy to prevent gender-based violence.

2021 General Assembly Resolution (A/RES/75/176)	It recognizes the importance of the right to privacy to prevent gender-based violence and calls for implementing and strengthening gender-responsive policies on privacy.
2021 The Committee on the Rights of the Child in its General Comment No. 25	It calls for the protection of children against technology-facilitated violence and online sexual exploitation and abuse.
2022 Report of the Secretary General on Intensification of efforts to eliminate all forms of violence against women and girls (A/77/302).	The Report (for which UN Women analysed data and coordinated information submitted by 35 Member States and around 10 UN agencies) is focused on the urgent need to address VAW in digital contexts and contains conclusions and specific recommendations for future action.
2023 The 67th session of the Commission on the Status of Women	It had as a priority theme 'Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls.'
(ongoing) The International Convention on countering the use of information and communications technologies for criminal purposes	The Convention is still under development. The latest version, which resulted from the April 2023 ad-hoc working group meeting, recognizes the specific gender dimension of cybercrime.

The **Council of Europe** has also been active in addressing CV. The main legal instrument is the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention). The **Istanbul Convention**[184] applies to all forms of violence against women, including domestic violence (Article 2). The EU acceded the Istanbul Convention in June 2023 (six years after its signature), triggering the entry into force of the convention for the EU on 1 October 2023.[185] Despite the EU's ratification, five EU Member States have not yet ratified the convention: Bulgaria, Czechia, Hungary, Lithuania and Slovakia.

While **the Convention does not refer to CVAW, its scope as defined in Article 2 extends to violence committed in online spaces and through ICTs**. Moreover, the articles on sexual harassment (Art. 40) and stalking (Art. 34) are applicable to CVAW. This is specified in the explanatory report of the Convention,[186] according to which Article 34 on stalking refers to 'the pursuit of any active contact with the victim through any available means of communication, including modern communication tools and ICTs' as unwanted contact'.

The Convention shall be interpreted in the light of the **GREVIO's General Recommendation n.1**[187] on the digital dimension of VAW. Even though this recommendation is not legally-binding, it is an important reference for state parties. With this recommendation, GREVIO intends to categorise manifestations of VAW in the digital sphere as expressions of GBV covered by the Istanbul Convention. GREVIO clarified through its General Recommendation No 1 that: (1) the definition of VAW set out in Article 3a covers many forms of VAW perpetrated online; and (2) the related requirements for state parties to establish legal and policy frameworks to tackle all forms of VAW should cover the forms of cyber violence.

However, the choice of addressing CVAW in a soft law instrument rather than a hard law one has been criticised. According to some academics, by doing so CVAW has been side-lined and excluded from the scope of a legally binding instrument. [188]

Other relevant CoE' instruments applicable to CVAW are summarised in the table below.

CoE instruments relevant to CV	Information
1981 The Council of Europe Convention 108+	The Convention regulates data protection. The scope of application of the protection includes both automated and non-automated processing of personal data and guarantees the protection of sensitive data such as genetic and biometric data as well as a 'right to erasure.'

2001 Budapest Convention on cybercrime and additional protocol	It is the first and most relevant regional legally binding treaty focusing on cybercrime and electronic evidence. The convention requires parties to criminalize offences perpetrated against or by means of computer data and systems, content-related offences pertaining to the production, distribution or possession of child sexual abuse material (CSAM) as well as infringements of copyright and related rights. The convention does not refer to VAW. However, some substantive criminal law provisions address directly and indirectly some types of CVAW.
2007 Convention on the Protection of Children against sexual exploitation and sexual abuse (Lanzarote Convention)	The Convention requires states to offer a holistic response to sexual violence against children through the '4 Ps approach': prevention, protection, prosecution and promotion of national and international cooperation. Articles 18 to 23 are relevant to CV.
2019 The Council of Europe Recommendation on preventing and combating sexism	It contains the first regionally agreed definition of sexism, including online and via new technologies, and reaffirms the existence of a continuum of violence affecting women and girls.
The Council of Europe Gender Equality Strategy 2018- 2023	The Strategy reaffirms the existence of forms of discrimination and violence affecting women's rights, safety and security online and offline. The Strategy highlights the idea of a continuum of VAW online and offline.
Gender Equality Strategy 2024-2029	The Strategy has six key priorities, including Preventing and combating VAW and Preventing and combating gender stereotypes and sexism. Under the latter category, the following sub-categories are relevant to CVAW: sexist hate speech (both offline and online) and women in media and AI.
The European Convention on Human Rights (ECHR)	CVAW can be considered a violation of: Article 8 – right to respect for private and family life; Article 10 – freedom of expression; and Article 14 – prohibition of discrimination of the ECHR.

2. EU LEVEL

As noted in Section 2.2, there is no harmonised legal definition of CVAW at European level. Apart from the recently adopted Directive on VAW and DV, there is no other instrument addressing CVAW specifically. However, there are a range of EU legal and policy standards, which are applicable to CVAW.

The Directive 2024/1385 on combating violence against women and domestic violence

The Directive 2024/1385 on combating violence against women and domestic violence, adopted by the EU Parliament and the EU Council in April 2024,[189] lays down minimum rules concerning the definition of specific criminal offences and penalties to address VAW. In particular, it contains four articles dedicated to CVAW: Article 5 on non-consensual sharing of intimate or manipulated material; Article 6 on cyber stalking; Article 7 on cyber harassment and Article 8 on cyber incitement to violence or hatred. The new Directive also sets out rights of victims of all forms of VAW or DV and provides for their protection.

According to EWL[190] and, as confirmed by the consulted stakeholders,[191] **the Directive can be considered as a significant step forward to better protect women and girls from VAW**. Likewise, academics emphasise that the Directive marks a significant improvement in seeking to introduce minimum rules regarding many forms of CV.[192]

Among its strengths, the Directive encompasses in **just one instrument** both offline forms of VAW and digital ones. This is a first attempt to regulate CV within the broader context ofGBV; the interconnections between VAW in the physical and virtual world are, thus,

acknowledged. Moreover, both forms where the victim usually knows the perpetrator (e.g. stalking, harassment) and where the victim does not know the perpetrator (e.g. hate, deep fakes etc.) are covered.

Among the various provisions reinforcing victim's rights, some come to attention. The Directive provides that Member States should allow victims to report the offense by both **in-person and online reporting** (Article 14 and Recital 30). Moreover, article 15 requires **adequate expertise** for investigation and prosecution authorities. Member States are also encouraged to cooperate with women's specialist services for the creation and revision of **guidelines for prosecutorial authorities and law enforcement**. Such revision is necessary where technological developments lead to new forms of CV (Recital 49).

In recognition of the increased risk of repeated, prolonged or even continuous victimisation caused by CV, the **prompt removal of harmful material** is foreseen in Article 23. In this regard, Member States should encourage the **self-regulatory cooperation between relevant intermediary service providers**. Self-regulatory measures should include the detection of systematic risks, the reinforcement of mechanisms to tackle CV and the improvement of training of moderators. Such measures complement action under the Digital Services Act (Article 23 and Recital 52).

Specialised support services for victims of CV are foreseen in Article 25. Besides, Article 34 lists among **preventive measures** the development of digital literacy skills whereas Article 36 requires that the training of professionals should be accompanied by follow-ups.

Other positive aspects of the Directive are the definitions of **cyber harassment and cyber stalking**. The former is broad enough to include cyber-harassment, mob attacks, cyberflashing and doxing; the latter contains the elements of repetition and continuity, which are key features of stalking behaviour. It also is important to acknowledge that according to Article 9, 'inciting' the commission of cyber harassment (Art. 7),[193] cyber stalking (Art. 6) and the non-consensual sharing of images are punishable as criminal offences (Art. 5).

Despite the above provisions, the **Directive is not without limits and has been subject to severe criticism**.

First, the **exclusion of the article on rape** from the Directive has been heavily criticised by the EWL[194] and other stakeholders. Considering the links between offline and online violence, this also concerns CV. Cases of CVAW include threats of rape and can end up with the tracing of the victim's location and her physical assault including rape (e.g. in the context of intimate partner violence or dating violence). The original draft of the bill, tabled by the European Commission in March 2022, included a definition of the crime of rape in alignment with the Istanbul Convention as sex without consent. However, after months of negotiations, 14 Member States continued to block the consent-based definition.

Cases of CVAW include threats of rape and can end up with the tracing of the victim's location and her physical assault including rape.

The exclusion of rape has been regarded as a big disappointment for the EWL and the majority of stakeholders, given its prevalence and the interconnections between CV and rape.[195] In this regard, the EWL analysed the definition of rape across the EU countries[196] and highlighted how this Directive would have led to a consent based definition of rape in several countries like Italy, France, Poland, Czechia, Bulgaria, Estonia, Hungary, Latvia, Lithuania, Romania and Slovakia.

Concerning the **articles 5-8 on CVAW**, some critical points have also raised concern among key players in this area. These articles on CVAW refer to **intentional conducts**. This reference poses some legal challenges given that the intentionality of the act must be proved. In criminal law, intent is the conscious decision someone makes to deliberately engage in an unlawful or negligent act, or to harm someone else. An act becomes criminal when taking into account the intent of the person who carries it out. **This indirectly places an 'onerous' burden of proof on victims of CV**, also considering the complexity of new technologies used to commit CV and the fact that victims may lack ICT skills.

Moreover, Articles 5, 6 and 7 also refer to '**serious harm**'. This reference raises questions on how harmful an aggression has to be to a victim for it to be considered a 'serious harm'; this formulation challenges the harmfulness of CV. According to some stakeholders, this is part of the broader problem of CV being perceived as 'not real', which forces the victims to prove the harmful consequences of the aggressions (see Section 4.1).[197] The 'serious harm' condition creates legal uncertainty for victims across and within countries leaving to judicial discretion the decision on whether these conducts are punishable.[198]

Furthermore, Articles 5 and 7 refer to making certain material accessible, through ICT to '**the public**'. Recital 18, in relation to article 5, leaves the interpretation of the term 'public' to the discretion of the judge according to the circumstances and the technologies used which might risk excluding, for example Whatsapp groups. Recital 26, in relation to article 8, instead states that 'public' should be understood as reaching an unlimited number of users. The broader term 'other end-users', as suggested by the EU Parliament, would have been preferable as made clear by EWL.[199]

Article 5 refers to the 'non-consensual sharing of intimate or manipulated material' whereas the broader term of 'image-based sexual abuse' is preferred by academics as well as by the EWL and other stakeholders.[200] The latter refers to all forms of the non-consensual creation, taking or sharing of intimate images or videos, including altered or manipulated media, and threats to distribute such material. It is 'umbrella' term capturing a range of interrelated forms of abuse, and not therefore limited to the non-consensual distribution of intimate materials. The term 'image-based sexual abuse' goes beyond distribution, to encompass the non-consensual creation of intimate images or videos, particularly using technology and AI to alter material to make it sexual and abusive, often known as 'deepfakes'.

Article 5(b) on non-consensual sharing of manipulated material has also a limited scope; it only applies to material where the person appears to be '**engaged in sexual activities**'. Therefore it excludes nudes, leaving out of the scope a large part of sexual digital forgeries. Beside what might constitute 'sexual activities' is likely to vary considerably across Member States and give rise to definitional confusion.[201] Likewise, **Article 5(c) on threats is not comprehensive** as it only includes where done so '**in order to coerce another person to do, acquiesce or refrain from a certain act**'. This will include coercive circumstances such as sexual extortion where a victim has already shared intimate images and the perpetrator threatens to distribute them, unless further intimate material is shared. However, it will not cover threats made with the aim of causing distress to the victim. For example, an ex-partner may threaten to distribute intimate images to deliberately cause distress, rather than to coerce the victim to do a particular act. Similarly, many other perpetrators may make threats for reasons not always apparent, but designed to cause direct harm, perhaps to exercise power and control over the victim, but without it being related to 'certain acts'.[202]

References to exceptions linked to '**freedom of expression**' and '**freedom of the arts and science**' in Article 5 and Recital 20 are also alarming as these could be used to justify the non-consensual sharing of intimate material. These inclusions might vanish the effectiveness of this article by leaving discretion of whether to criminalise non-consensual sharing of intimate images or not, to the judicial authorities. According to EWL, the notion of freedom of expression should not become a way to justify online hatred and gender discrimination.[203]

As for article 8 on cyber incitement to hatred or violence, the following paragraph allowing Member States to limit the scope of this article has been introduced: 'For the purpose of paragraph 1, Member States may choose to punish **only** conduct which is either carried out in a manner **likely to disturb public order or which is threatening, abusive or insulting**. Moreover, recital 18 specifies that 'public' should be understood as a **potentially unlimited number of persons**. This limits considerably the applicability of the provision, leaving the punishment of the conduct to the discretion of judicial authorities.

Finally, Recital 21 on cyber stalking states that there may be **some circumstances in which surveillance is carried out for legitimate purposes**, such as parents monitoring the online activity of their children or caregivers monitoring the health of those in their care. It should be taken into account that in the context of intimate partner violence tools used to monitor children have been weaponized by perpetrators to continue coercive control.[204]

Other forms of CV, such as **new forms perpetrated through artificial intelligence**, apart from deep fakes, that are increasing (see Section 2.3) are not expressly mentioned in the articles on CV but only generically cited in Recital 19.

In addition to the Directive, **other EU instruments** apply directly or indirectly to CVAW; these are presented in the sections below.

The Victim's Rights Directive

The **Victim's rights directive**[205] (Directive 2012/29/EU), (hereafter referred as VRD) is the core EU level instrument that lays down a set of rights for all victims of all crimes and imposes corresponding obligations on Member States. The Directive states that all victims of crime and their family members are to be recognised and treated in a respectful and non-discriminatory manner based on an individual approach tailored to the victim's needs. It provides victims, among others, with a right to information, a right to understand and be understood, a right to access support and protection in accordance with their individual needs, as well as with a set of procedural rights. The Directive protects victims of crime as defined under national laws. It is therefore applicable to forms of CVAW that are criminalised in Member States.

The Directive is currently under revision.[206] The proposed revision, included in the EU strategy on victims' rights (2020-2025),[207] aims to address the key issues identified in the evaluation of the VRD.[208] The evaluation highlighted some challenges in identifying a crime. While some crimes are easier to identify and establish, some offences and damages are intangible and therefore difficult, if not impossible, to prove. This is particularly the case for crimes committed using new technologies, such as cybercrime and online harassment. Stakeholders reported that in such cases the relevance of the current provisions of the Directive can be questioned. It was noted that new technologies also bring with them a higher risk of re-victimisation (harmful content online may be difficult to remove or may reappear). Moreover, the evaluation stressed the absence of provisions on the removal of illegal content online, notably child sexual abuse and cyberbullying material leads to secondary victimisation.

The update of the VRD represents a unique opportunity to address the rights of victims of CV, in particular women. It remains to be seen whether the revised Directive will make express reference to CVAW. The EWL is also advocating for the revision of the VRD to include a specific support to women victims of different forms of violence.

The Directive on preventing and combating trafficking in human beings and protecting its victims

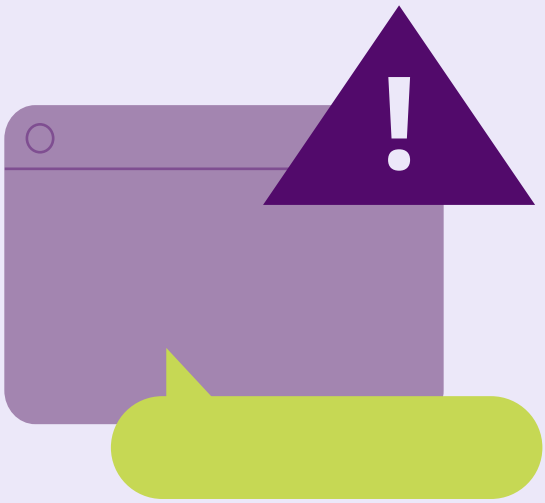
The Directive on preventing and combating trafficking in human beings and protecting its victims [209](Directive 2011/36/EU) has recently been reviewed.[210] In April 2024, the European Parliament voted in favour of the updated version of the Directive that includes forced marriage, illegal adoption, exploitation of surrogacy and a better support for victims.

As explained in the explanatory memorandum of the proposal, the updated Directive partially recognises the online dimension of trafficking. Trafficking in human beings committed or facilitated through ICTs, including internet and social media, is now considered an aggravating circumstance when it relates to sexual exploitation, leading to higher penalties. Thus, the non-consensual dissemination of videos and images of a sexual nature can be taken into account by judicial authorities as an aggravating circumstance.

This is an important step forward given that new digital technologies are widely used to reach out to potential victims. Already, in its 2019 Conclusions on combating the sexual abuse of children,[211] the Council had stressed the increasing and aggravating role of digital technologies. According to the Council, the internet has created unprecedented opportunities for abusers and criminals for the distribution, trade, possession, and viewing of women sexual abuse material and child sexual abuse material. Likewise, in 2020, a Europol report[212] had focused on the challenges of countering human trafficking in the digital era.

The report highlighted the advantages offered by new technologies for traffickers: anonymity, scope for outreach, capacity to control victims even at distance. It outlined the various strategies used by traffickers to detect, attract, recruit and control victims through digital technologies. Those technologies have changed the geographical scope of intervention of traffickers, their 'business model' and even their internal structure of work.

The Digital Services Act



The **Digital Services Act** [213](DSA), adopted in October 2022, aims to create a safer online environment for consumers and companies in the EU. It sets rules designed to: define clear responsibilities for online platforms and social media; deal with illegal content and products, hate speech and disinformation; as well as achieve greater transparency with better reporting and oversight.

The DSA introduces responsibilities and a system of accountability and transparency for providers of intermediary services, such as: internet access providers, online marketplaces, social networks, content-sharing platforms etc. The regulation also includes special rules for very large online platforms (VLOPs) and very large online search engines (VLOSEs). In this regard, the DSA has the following specific objectives:

1. Combat illegal content online;
2. Empower users by giving them ability to challenge content-moderation decisions and seek redress; grant authorities access to key data generated by the VLOPs to gauge online risks and require transparency on a range of issues, including algorithms;
3. Set obligations for VLOPs and VLOSEs to prevent their systems being misused (e.g. safeguards for children and limits on using sensitive personal data for targeted advertising);
4. Reinforce supervision and enforcement of all intermediary service providers.

In particular, the DSA stipulates that intermediary providers, which moderate user-generated content, must make transparent which moderation rules apply, and which measures they implement to enforce these.[214] It also stipulates that platforms using a notice-and-takedown-procedure must create a system by means of which illegal content can be reported. Platforms above a certain size must implement a procedure by which those affected can appeal against any blocking. Moreover, all providers must ensure transparency about any blocking that has taken place (information on the reason for blocking and the respective complainant).

To this end, providers of intermediary services and online platforms must publish **periodic transparency reports on content moderation**. These reports must include information such as the number of orders providers have received from Member States' judicial or administrative authorities, the human resources dedicated to content moderation, the number of accounts and items of content taken down voluntarily by the provider, and the accuracy and rate of error of their automated content moderation systems. Besides, the DSA makes **express reference to**

GBV. It requires VLOPs to assess systemic risks stemming from their design or the functioning of their services; this includes risks in relation to fundamental rights and GBV as manifested online. In particular, according to Article 34 providers of VLOPs and VLOSEs shall diligently identify, analyse and assess any systemic risks stemming from the design or functioning of their service and its related systems, including algorithmic systems. This risk assessment shall include the following systemic risks: any actual or foreseeable negative effects in relation to GBV (Art. 34(1)(d)).

Moreover, **Article 35** requires providers of VLOPs and VLOSEs to put in place **reasonable, proportionate and effective mitigation measures**, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include adapting content moderation processes, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular in respect of **illegal hate speech or CV**, as well as adapting any relevant decision-making processes and dedicated resources for content moderation (Art. 35(1)c)).

Further references to CVAW are contained in the Preamble. Recital 12 specifies that the concept of '**illegal content**' under this Regulation should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as **illegal hate speech**, or that the applicable rules render illegal in view of the fact that it relates to illegal activities such as the **sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking**.

Furthermore, according to Recital 87, providers of VLOPs, in particular those primarily used for the dissemination to the public of pornographic content, should diligently meet all their obligations under this Regulation in respect of **illegal content constituting CV**, including illegal pornographic content, especially with regard to ensuring that victims can effectively exercise their rights in relation to content representing **non-consensual sharing of intimate or manipulated material** through the rapid processing of notices and removal of such content without undue delay.

In addition to Article 34 mentioned above, the DSA includes other provisions assessing the **fundamental rights compliance of online platforms** such as: [215]

- Terms and conditions with due regard for fundamental rights, including restrictions imposed on service use in light of the freedom of expression, freedom and pluralism of the media and other rights enshrined in the Charter of Fundamental Rights of the European Union (Article 14 of the DSA);

- Recommender system transparency, especially in view of the main parameters that lead to content recommendations (Article 27);

- Data access and scrutiny to allow for external scrutiny of the societal and fundamental rights risks of online platforms (Article 40). In Chapter IV, the DSA outlines the framework for

The DSA can be considered a step forward to better protect users in the digital space

enforcement, implementation, cooperation and sanctions. The European Commission has significant supervisory and empowerment powers, together with the National Digital Service Coordinators and the European Board for Digital Services. In particular, the Commission is the primary regulator for VLOPs and VLOSEs; the centralised approach is set due to the potential cross-border impact in case of failure to comply with the DSA obligations. The Commission has the following competences:

- Exclusive powers for provisions in Section 5 of Chapter III: the due diligence obligations, including risk assessments, independent audits, and additional online advertising transparency;

- Investigative powers, exercised either through its own initiative or at a request of a national Digital Service Coordinator (DSC) upon suspicion of infringement by VLOPs or VLOSEs;

- Enforcement powers, including the request to provide information, issue non-compliance decisions, impose fines and make legally binding commitments.

Moreover, Articles 49 and 50 establish that the enforcement of the DSA is primarily in the hands of the Member States, which are obliged to designate at least one authority as the **Digital Services Coordinator** (DSC) to be responsible for the supervision of the digital intermediary service providers and the enforcement of the DSA. The national DSC has: vast investigation powers, including carrying out on-site inspections and requiring the production of documents and information; is responsible for coordinating the enforcement of the DSA; has extensive enforcement powers, including making compliance agreements, imposing interim measures, fines and penalties. Finally, the **European Board for Digital Services (EBDS)** is an independent advisory group aimed at supporting consistent application of the DSA. It comprises all DSCs who have voting power, and the Commission as a chair, without voting power.

As confirmed by the stakeholders consulted for this Report,[216] **the DSA can be considered a step forward to better protect users in the digital space**. According to academics, the measures in the **EU's Digital Services Act are a welcome recognition of the prevalence and harms of image-based sexual abuse.**[217] In particular, in seeking to reduce, and ultimately prevent, many cases of such abuse, these provisions tackle the core of the problem.

GBV is recognized as one of the macro area of risks along with other risks (e.g. disinformation, the impact that the digital can have on political elections, children's protection, the impact on mental and body health). Within the macro area of GBV, **specific categories are now in the process of being created by the Commission under the 'Transparency Reporting Package'**.[218] These sub-categories correspond to the forms of CV that can be reported by users such as: cyber stalking, cyber harassment, cyber flashing, hate, non-consensual images etc. This represents a positive development, although it remains to be seen which sub-categories will be created in practice and to which extent the forms of CVAW will be covered effectively.

Another positive development under the DSA is the fact that the **Commission designated under the Regulation three porn platforms (Pornhub, XVideos and Stripchat) as Very Large Online Platforms (VLOPs)** in December 2023.[219] The designation comes with heightened responsibilities regarding transparency and child protection. It will allow for higher scrutiny and accountability of the platforms' algorithms and processes. As explained under Section 2.3, there has been an increase in deepfakes sexual abuse, thus, the designation will ensure more control over pornographic material and better protection of women.

Despite these positive developments, **the DSA has been subject to some criticism**.[220] According to experts from the Durham and Essex Universities,[221] the DSA fails to recognise the **gendered nature of harm**. The DSA does not expressly define the harms within scope; it cross-refers to relevant EU legislation and the various national legal systems. It has been well recognised that there is a gendered risk of harm, and that intimate image abuse is a central part of that problem. It is, therefore, important that this particular issue is expressly addressed to ensure that formal neutrality does not in practice disadvantage already minoritised groups.[222]

According to Turillazzi A. et al.[223] **different regulatory approaches should be implemented to illegal and harmful content**. In the DSA, there is no clear definition of what is harmful and what is illegal. This is problematic in the EU context, given that some contents or behaviours may be illegal in some Member States, and 'not-illegal-but-harmful' in others. Similarly, Stringhi[224] criticises the **definitional weaknesses of due diligence provisions**. While, in theory, the DSA has the potential to improve responses to CV, she questions whether the DSA is a significant step-forward, suggesting, instead, that the absence of a regional understanding of illegal content renders the DSA almost unfit for purpose in the face of digital and online violence. Allen points out that very large online platforms and search engines should prioritise transparency and meaningful consultation with civil society as they fulfil their mandatory due diligence obligations, in particular those around risk assessment and mitigation.[225]

Problematics related to the effective application and enforcement of the DSA will need to be looked at in the future. According to stakeholders, more much needs to be done to make sure that online platforms, including porn companies, meet their obligations under the DSA[226] (see Section 4.8).

The Artificial Intelligence Act

The **Artificial Intelligence Act** (AI)[227] was adopted by the European Parliament on 13 March 2024. The AI Act takes a risk-based approach to safeguard fundamental rights, democracy, the rule of law, and environmental sustainability. The Act distinguishes between 'unacceptable risk', 'high risk', 'limited risk' and 'minimal risk'. It bans the use of AI systems that pose an unacceptable risk to the safety and fundamental rights of EU citizens. For AI systems that fall into the high-risk category, providers would be obligated to carry out risk-assessments, provide for documentation and human oversight, and ensure high-quality datasets, among other requirements. For certain, AI systems, only minimum requirements are formulated, while applications that represent minimal risk are not regulated.

It is important to note that the Act allows for the use of **'deepfake' technologies** but foresees some **minimum requirements in relation to transparency obligations**. Creators of sexual digital forgeries (known as 'deepfakes') are obliged to label their content so that it should be clear to anyone that they are dealing with manipulated material. Specifically, article 52 (3) provides that they 'shall disclose that the content has been artificially generated or manipulated'. Some exceptions to this provision apply: where the use of manipulated content is authorised by law; and where the content forms part of an artistic work. In the latter case, the transparency obligations are limited to disclosure of the existence of such manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work.

As noted by the EPRS' study,[228] while a labelling obligation for sexual digital forgeries[229] could be a first step, **the nature and scope of this measure remains unclear**. Firstly, the act does not include concrete guidelines for such disclosure. It also remains to be seen if malicious actors, who often distribute sexual digital forgeries anonymously, will even be affected by these requirements.

While the Act represents an opportunity to mitigate some of the risks posed by the misuse of AI such as deep fakes, it **does not contain any express reference to CVAW**. Moreover, the Act refers to **gender equality** only generically, as confirmed by the consulted stakeholders.[230] Such reference is included in Article 69(2)(e) on voluntary codes of conduct. The inclusion of certain aspects as voluntary measures within the Act, including Article 69, raises significant concerns according to feminist organisations. This approach falls short of ensuring a robust and gender-equitable implementation that feminist principles demand.[231]

Other references to gender equality are contained in the Preamble. Recital 28(a) clarifies that the extent of the adverse impact caused by the AI system on the fundamental rights - including gender equality - is of particular relevance when classifying an AI system as high-risk. Recital (14) states that diversity and non-discrimination means that AI systems are developed and used in a way that promotes equal access and gender equality. Other references are included in Preamble 37 and 81.

The **lack of a comprehensive gender dimension** with the text has been highlighted by the Special Committee on Artificial Intelligence in a Digital

Age of the European Parliament.[232] The latter underlines the gender gap across all digital technology domains, which has a concrete impact on the development of AI, reproducing and enhancing stereotypes and bias, since it has predominantly been designed by males. This has the potential to deepen already existing inequalities as well as to lead to a devaluation of problems that affect mostly women, such as CVAW.

The General Data Protection Regulation

The **General Data Protection Regulation**[233] (Regulation (EU) 2016/679) protects individuals when their data is being processed by the private sector and most of the public sector. The Regulation offers the potential to cover some aspects of CVAW, as it demands, for example, that companies integrate privacy by design into their products or that individuals responsible for uploading image-based sexual abuse material as well as publishers of such material are considered joint data controllers and hence fall under the obligations and sanctions imposed by the GDPR. Moreover, the GDPR also contains a 'right to erasure,' better known as the right to be forgotten. However, **the regulation does not define any form of CV, but it provides protection to victims of CV** (e.g. victims of non-consensual sharing of intimate images) **and provides for sanctions to be imposed against the individual responsible for sharing the unconsented content and against the publisher of such material.**[234]

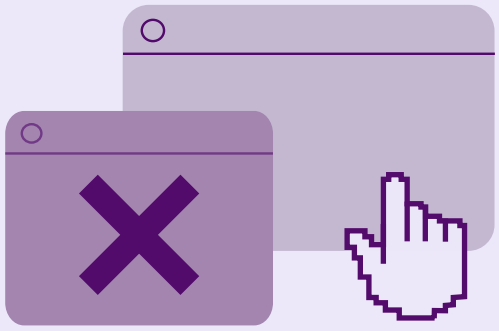
With regards to sexual digital forgeries ('deepfakes'), a sexual digital forgery that depicts a natural person can be considered personal data under the GDPR, since it relates to an identified or identifiable natural person. **The GDPR is, thus, applicable to the development of 'deepfake' software and applications, and to the creation and dissemination of sexual digital forgeries**. The GDPR provides that the processing of personal data always require a legal basis.

There are six possible legal grounds for the processing of personal data, but only 'informed consent' and 'legitimate interests' are likely to qualify within the context of digital forgeries (deepfakes). When the creator of a 'deepfake' claims to have a **legitimate interest for processing someone's personal data, the legitimate interests pursued by the creator may not be overridden by the interests or fundamental rights and freedoms of the person depicted**.[235] This could be the case, for example, with an ironic digital forgery depicting a famous person. In such a case, the creator could claim the right to freedom of speech for

purposes of satire or political commentary. **This would be particularly dangerous for women in the public eye such as politicians or journalists who are often the targets of CV** (see Section 2.6) as the freedom of speech could be used to justify sexual digital forgeries against them.

When legitimate interests are not applicable, the use of personal data for the creation and dissemination of digital forgeries needs to be subjected to informed consent by the persons depicted in the video (both the person(s) in the original video and the person(s) who appear in the fabricated video), as the personal data of all of them are processed. If creators of a digital sexual forgery fail to obtain prior consent, they are at risk of violating the GDPR.

Moreover, the **GDPR provides victims with the right to correct inaccurate data, or even have it deleted. Within the context of sexual digital forgeries (deepfakes), however, the legal route for victims can be challenging**. In many cases, it will be impossible for the victim of CVAW to identify the perpetrator, who often operates anonymously. Moreover, victims might lack the appropriate resources needed for starting a judicial procedure, leaving them vulnerable.



Other EU instruments applicable to CVAW

Other EU legal instruments that could apply to CVAW are summarised in the table below.

EU instrument	Information
Media Freedom Act 2024	The Media Freedom Act - first proposed by the EU executive in September 2022 – was adopted on 13 March 2024. The Act will oblige EU governments to better protect media against malign interference and limit the use of spyware against journalists. The Parliament had hoped the law would introduce a full ban on the use of spyware against reporters. However, a handful of Member States - including France, Italy, Malta, Greece, Cyprus, Sweden, and Finland - had pushed for an exemption. EU governments will be able to use spyware against reporters as a 'last resort' mechanism where there is a legal motive. While this represents a step forward for women journalists who are often targets of CVAW, the use of spyware will still be possible and could limit their freedom of expression.

Directive on child sexual abuse (Directive 2011/93/EU)	It aims to protect minors from non-consensual intimate image abuse (considered CSAM when the victim is a minor). Article 25 obliges EU Member States to promptly remove child abuse materials within their territory and to endeavour to secure the removal of materials hosted elsewhere, offering the possibility to block access to CSAM. The Directive might be replaced by the Regulation on Child Sexual Abuse Material (CSAM) and currently under negotiations recasting Directive 2011/93/EU, both.
Audiovisual media services directive (Directive 2010/13/EU)	The AVMSD contains several guidelines on preventing harm, especially drawing attention to the protection of the wellbeing of minors. Member States are directed to regulate video-sharing services in order to prevent impairment of the physical, mental or moral development of minors and to offer effective parental controls. Pornography and violent content should be treated by the strictest measures, such as age-verification, PIN-codes, clear labelling or automatic filtering. The AVMSD calls for regulations that require video-sharing platforms to detect the nature of the content shared and implement measures in the interest of the viewer, creator and general public. The AVMSD thus contains provisions to respond to, for example, the distribution of sexual digital forgeries (deepfakes). The Directive recognises that Member States will have to balance the regulation of harmful content with applicable fundamental rights, such as the freedom of expression and respect for private life.
Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.	The Decision requires the criminalisation of public incitement to violence or hatred based on race, colour, religion, descent or national or ethnic origin. Certain forms of conduct as outlined below, are punishable as criminal offences: • Public incitement to violence or hatred directed against a group of persons or a member of such a group defined on the basis of race, colour, descent, religion or belief, or national or ethnic origin; • The above-mentioned offence when carried out by the public dissemination or distribution of tracts, pictures or other material; -publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes. The Decision does not make reference to gender/women nor to cyber-crimes. In 2021, the European Commission adopted a Communication, which prompted a Council decision to extend the current list of EU crimes to hate crime and hate speech. If this Council decision is adopted, the EC could propose a criminalisation of hate speech and hate crime also on the basis of gender. While the Parliament supported the Commission's proposal and endorsed its version of the text in plenary in January 2024, the EU Council is not advancing as unanimity is required to move forward.

Recast directive on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (Directive 2006/54/EC)	The directive could apply to some forms of CVAW. However, it does not explicitly mention the online aspects and it is limited to matters of employment and occupation. The revision of the Directive is currently under negotiations and considering the changing of legislature after the 2024 EU elections it is yet unclear what direction the negotiations will take.
Directive on e-commerce (Directive 2000/31/EC)	It obliges service providers to remove or disable access to illegal content hosted on their platforms. Concerning sexual digital forgeries, in principle, the e-Commerce Directive already enables the removal of illegal 'deepfake' content. However, it does not contain a clear definition of what exactly is meant by illegal content. Furthermore, the Directive harmonised the conditions for releasing providers from liability, but not the conditions that must be met in order to establish liability. The Commission recognised as early as 2012 that harmonisation in this area was insufficient, but until recently it refrained from regulatory measures and focused on encouraging self-regulation by platforms. In addition to the e-commerce Directive, since 2023 the Digital Services Act, as extensively explained above, forces platforms to remove illegal content and publish periodically transparency reports.
e-Privacy Regulation (not adopted yet)	The proposed regulation should lead to improved online privacy, particularly considering online interactions between citizens and businesses, and thus provide greater protection to women and girls.

EU non-legislative initiatives relevant to CVAW

At the **policy level**, various initiatives have been taken in this area over the years, most of them precede the legislative initiatives examined in the previous sections. On 14 December 2021, the European Parliament adopted a legislative-initiative resolution,[237] recommending that the European Commission use its forthcoming proposal for a directive on combating GBV to criminalise gender-based CV, as a cornerstone for the harmonisation of existing and future legal acts. On the same year, two additional resolutions, relevant to CV were adopted (**resolution on children's rights** in view of the EU strategy on the rights of the child;[238] and the **2021 resolution on the implementation of Directive 2011/36/EU** on preventing and combating trafficking in human beings and protecting its victims).[239] These were preceded by the **2020 resolution on strengthening media freedom** focusing on the protection of journalists, hate speech, disinformation and the role of platforms.[240]

Moreover, the EU Parliament published a **resolution in May 2021 on 'Artificial intelligence in education, culture and the audiovisual sector'**.[241] This resolution aimed to: stress the importance of raising awareness of the risks of sexual digital forgeries (known as 'deepfakes') and improving digital literacy (No 90); address the increasing difficulty of detecting and labelling false and manipulated content by technological means (No 91); call upon the Commission to introduce appropriate legal frameworks to govern the creation, production or distribution of sexual digital forgeries for malicious purposes (No 91); promote the development of detection capabilities (No 92); improve transparency with regard to what content is displayed to platform users and give them greater freedom to decide whether and what information they want to receive (No 93).[242] Moreover, in a **2020 report** on the intellectual property rights for the development of artificial intelligence, the Parliament called for increased awareness-raising and media literacy, in order to combat the possibility of mass manipulation through sexual digital forgeries.[243]

In turn, the **European Commission** has put forward a range of policies relevant to CVAW, such as the gender equality strategy 2020–2025,[244] the strategy on victims' rights 2020–2025,[245] the strategy for a more effective fight against child sexual abuse 2020–2025,[246] the EU cyber security strategy[247] and the EU strategy on combating trafficking in human beings.[248]

Furthermore, other voluntary initiatives on **sexual digital forgeries** have been taken by companies and EU political parties. In February 2024, 20 tech companies, including Amazon, Open AI, Snapchat, Microsoft, Google, Tik Tok, announced a new Tech Accord[249] to combat deceptive use of AI in 2024 Elections. In April 2024 during a ceremony at the Commission, the major EU's political parties - the European People's Party (EPP), the center left Party of European Socialists (PES), and the right wing European Conservatives and Reformists Party (ECR) - signed a voluntary code of conduct[250] ahead of the European election to avoid making and spreading unlabelled sexual digital forgeries.

The Parliament called for increased awareness-raising and media literacy, in order to combat the possibility of mass manipulation through sexual digital forgeries.

Other measures, only indirectly related to CVAW, were adopted to **tackle disinformation** after the start of the Russian war against Ukraine in 2014. These initiatives included: the European Parliament's resolution of 2017 on online platforms and the digital single market,[251] which urged the Commission to adopt hard regulatory means to deal with fake news; a public consultation of the Commission on fake news in late 2017[252] and the appointment of a High-Level Expert Group on Fake News and Online Disinformation in early 2018.[253]

These steps led to the publication of the **Code of Practice on Disinformation** in 2018.[254] In addition to measures such as closing fake accounts, a key component of the Code was online political advertising. This was to be achieved by platform operators making a distinction between political and non-political content. The Code is relevant to women politicians who are the main targets of CV (see Section 2.6). The Code was signed by Mozilla, Twitter, Facebook, Google in October 2018. Microsoft and TikTok joined in 2019 and 2020, respectively. Several studies, however, indicated that the Code was lacking a meaningful possibility to measure its effectiveness, and that the published transparency reports often did not contain important information. As a result, the effectiveness and efficiency of the Code itself was called into question.[255]

The **EU code of conduct on countering illegal hate speech online**[256] should also be mentioned. To prevent and counter the spread of illegal hate speech online, in May 2016, the Commission agreed with Facebook, Microsoft, Twitter and YouTube this code of conduct. In the course of 2018, Instagram, Snapchat and Dailymotion took part to the Code of Conduct, TikTok in 2020 and LinkedIn in 2021.[257] The implementation of the Code of Conduct is evaluated through a regular monitoring exercise set up in collaboration with a network of organisations located in the different EU countries. **The code of conduct has a strong focus on tackling racist hate speech, being an outgrowth of the 2008 Framework Decision on combating certain forms and expressions of racism and xenophobia,[258] and does not explicitly address gender-based hate speech**. Moreover, as pointed out by the consulted stakeholders, the Code would benefit from a review to incorporate a gender dimension and in light of new technological developments. It is clear at the outset that the Code fails to address gender-based violence on digital platforms.

3. NATIONAL LEVEL

Given the limited timeframe and the small size of the Report, it was not possible to conduct a full review of national legislation for all Member States. However, a concise overview of the national legal frameworks, including recent initiatives, is provided in this section.

According to CoE, some Member States have taken important steps to prevent and combat certain aspects of CVAW in the last five years.[259] Initiatives aimed to introduce new criminal offences or extend existing ones to regulate specific acts of violence or harmful behaviours perpetrated online or through technology. For example, in **France**, cyberbullying against women and girls has been introduced as a new criminal offence. In **Slovenia and Poland**, legislation criminalises both offline and online manifestations of stalking. **Italy** introduced a new criminal offence: the unlawful dissemination of sexually explicit images or videos. In **Austria**, an online hate speech package (Hass im Netz) provides new tools to address it. In **Estonia**, a 'web constables' unit in the police which specialises in handling hate speech and harassment online, was created whereas in **Ireland**, the 2021 Bill on Harassment, Harmful Communication and Related Offenses criminalised all forms of non-consensual sharing of intimate images, with penalties up to 10 years in prison.[260]

Recent developments have also occurred in **Belgium, Croatia, Greece and Malta**. Most of the new measures concern cyber harassment, cyber bullying, online hate speech and non-consensual intimate image abuse.

Initiatives vary according to the specifics of each national legal system. As noted in EIGE's 2022 report,[261] CV is regulated in four different ways across Member States:

1. CV is punished as a specific offense;
2. CV is an aggravating circumstance of general offenses;
3. CV is covered under general offences which refer to 'any means', including ICT means;
4. CV falls under general offenses with no reference to ICT or other means.

In most Member States **general offences** cover both offline and online/digital forms of CV. For example, the offences of stalking and harassment apply to stalking and harassment committed in the physical world and in the cyber world. However, these general offences lack a gender dimension.

Only one Member State has **specific legislation** on CV as a whole phenomenon: Romania.[262] The latter has adopted a **broad definition of CV** covering various forms: online harassment, online incitement to hate messages, online stalking, online threats, publishing information or content having a graphic intimate nature without consent, illegal access to intercepted communication and private data and any other form of abusive use of information technology and communications. However, reference to **gender** is only made with regards to online incitement to hate messages. Besides, CV is not criminalised; the victim can ask for civil protection.

Other Member States have adopted **legislation covering only specific forms of CV** (for example ad-hoc laws on cyber bullying and cyber harassment exist in Greece, Italy, Cyprus and Slovenia). With regards to the latter, a gender dimension is present in the Cypriot and Maltese legislation.

Finally, as highlighted by CoE, in several countries the issue of CVAW is only **partially tackled through the lens of Internet safety or children's protection**.[263] The recognition and sanctioning of the harm perpetrated against women and girls online mostly focuses on ensuring the person's safety, reputation or property, **failing to place it in the context of a continuum of violence and to capture other impacts** of such acts, including the social, economic, psychological and participatory harm.

Outside the EU, the **UK has recently adopted new initiatives to criminalise cyberflashing and more generally illegal content online**. The Online Safety Act, which gained Royal Assent late in 2023,[264] is a set of laws aimed to protect children and adults online. Platforms are required to promptly remove Illegal content which includes: child sexual abuse; controlling or coercive behaviour; extreme sexual violence; hate crime; inciting violence; revenge porn etc. Moreover, new offences, as part of the Online Safety Act, have been introduced in January 2024 to criminalise **cyberflashing and epilepsy-trolling**. Criminals will now face up to five years in prison for engaging in a range of online abuse, trolling and predatory behaviour.[265]

IV. Key challenges

The challenges to tackle CVAW are various and are classified in different categories; these are presented on next pages.

1. UNDERESTIMATION, LACK OF AWARENESS AND UNDER-REPORTING

The lack of awareness and the underestimation of the seriousness of online/digital violence are major issues that contribute to the **under-reporting of incidents**. In general, **CV is perceived as less severe and less harmful than offline violence**, despite its detrimental consequences (see Section 2.8).[266] Besides, very often women are not aware that the harmful experiences to which they are exposed online or through digital means are forms of violence. Many women are also unaware that they have been victims of image-based sexual abuse, particularly sexual digital forgeries and forms of voyeurism with hidden cameras, or where material is shared in groups and internet fora where victims are unaware their material has been distributed.[267]

According to a survey by UN Women, other **reasons for not reporting** are: the belief that nothing will be done, lack of trust in institutions, fear that confidentiality will not be respected and fear that they will be blamed for the experience. Only few of the surveyed women, reported cases of violence to the police (7.1%) or other institutions (4.5% to human rights institution, 2.6% to educational facility), and even less so to non-governmental organisations (2.5%); less than half of women reported their experience to friends or family (43.8%).[268]

Likewise, the EPRS's study notes that there are **several issues, which contribute to under-reporting**, some apply to both VAW and CVAW. The shame from being a victim can prevent women from disclosing their experiences. In certain countries, some women are embarrassed to talk about their experiences because of cultural norms. Cultural norms also mean that women may have a narrower definition of what

can be considered CVAW and are less likely to report incidents.[269]

Moreover, victims tend to believe their experiences will not be taken seriously. The fact that **law enforcement often does not have the tools or training** to properly handle CVAW cases (see Section 4.7) can worsen this belief. In some cases, victims prefer to avoid feelings of disempowerment.[270] When victims do report to social media platforms or law enforcement, only a small percentage of cases are pursued, and victims often do not receive follow-up information as to why.[271]

The underestimation, the lack of awareness and under-reporting of incidents of CVAW make it a challenge to understand the true extent of the problem and lead to an **underestimation of its prevalence**.

2. LACK OF HARMONISED DEFINITIONS

As mentioned in Section 2.2, there is a lack of a shared operational definition of CVAW across countries and key actors.[272] The review conducted by UN Women found that there is the **lack of a consistent and standard definition of TFVAW** as an umbrella term among stakeholders, as well as a lack of common vocabulary on its forms and modes. For example, it is not clear how to categorize different tactics or manifestations of TFVAW, or how to understand the different 'spaces' where TFVAW occurs.

At EU level, while several instruments are directly or indirectly applicable to CVAW (see Section 3.2), there is **not yet a harmonised definition of CVAW**.[273] Legal and statistical definitions of CV vary greatly across Member States and organisations. Moreover, most definitions are **gender-neutral and do not acknowledge the links between online and offline violence**.

In this regard, the Directive on combating VAW and DV is a step forward. However, it does not provide a definition of CVAW itself but focuses on specific forms: cyber harassment, cyber stalking, non-consensual sharing of images and hate speech (see Section 3.2).

The lack of a EU harmonised definition of CVAW has several implications, including the **lack of comparable data on CVAW across Member States** (see Section 4.5).

3. DISCREPANCIES AMONG THE LEGAL & POLICY FRAMEWORKS

As explained in Section 3.3, **the legal and policy frameworks on CV vary greatly across Member States**. While in the majority of Member States CV is covered under general offences, only few Member States have adopted specific laws on CV; however, the latter lack a gender dimension and apply only to specific forms of CV.

This is not only an issue at EU level. According to a review of legal frameworks by the UN, current laws on digital violence across countries lack clear and consistent definitions.[274] Some states have started to update their legal frameworks but there remain significant gaps and inconsistencies in the forms of CVAW that are covered and the remedies that may be accessed.[275]

Moreover, **different policies apply to internet intermediaries at international level**. The latter are responsible for preventing and detecting online VAWG with **little independent oversight, unclear standards that differ between platforms and that are inconsistently enforced** making it very difficult for victims to access support and protection. Another challenge that needs to be addressed is that the internet is borderless and, in many cases, online VAWG encompasses multiple offenders, **multiple victims across multiple platforms across different jurisdictions**.[276] The cross-border nature of CVAW and the intrinsic jurisdictional complexities have been highlighted by the consulted stakeholders.

The great variety of legal and policy frameworks affects the certainty of victims' rights; victims are entitled to very different civil and criminal remedies across countries. **This is an issue considering the transnational nature of CVAW**. Given that legal definitions are also used for statistical purposes (administrative data and surveys can be based on legal definitions), their differences across Member States affect the comparability of data on CVAW.

Moreover, although legislation to criminalise at least some forms of cyber violence is in place in some Member States, in some countries the **law places the burden of proof on victims**. The latter must prove they have suffered harm through expert reports. Besides, some national criminal laws also require **evidence of the intent to cause harm or emotional distress to the victim**, which may be difficult to prove, making convictions harder to achieve.

4. OUTDATED LEGISLATIONS

Considering the rapid evolution of technology, **legal frameworks on CVAW tend to become outdated very quickly**. While some countries are reforming their legislation, laws and regulations continue to lag significantly behind technological innovation.[277] Indeed, outdated legislation often struggles to keep up with the rapid pace of technological advancements. As technology evolves, new challenges emerge, and existing laws may become ineffective or insufficient in addressing them. By the time a regulation is finalised, the technology it aims to govern may have shifted or transformed significantly. This phenomenon is particularly evident in areas like social media.[278] As confirmed by stakeholders, legal frameworks are obsolete in relation to new forms of CVAW such as those facilitated by artificial intelligence. This problem could in part be tackled by adopting an uniform and comprehensive definition of CVAW (see Section 6).

5. CHALLENGES RELATED TO THE MEASUREMENT OF CVAW

At **EU level**, there is a high degree of **variety, overlap and disharmony of statistical definitions** across Member States.[279] The lack of harmonised statistical definitions is directly related to the fact that most Member States **do not collect data consistently**. Where data is collected, **it is not disaggregated by sex and is limited to very specific forms of CV**.[280] The **lack of common indicators** for statistical purposes is also a major problem, to which EIGE is responding.

Likewise, at **international level**, the lack of data on the digital dimension of violence against women is exacerbated by the fact that existing **data is often not disaggregated** by sex, age, relation between the victim and the perpetrator, disability or other relevant factors.[281] This gap may be due to a range of factors including the lack of consideration of the digital dimension in national statistics on violence against women and girls; the absence of statistics disaggregated by sex on the incidence of computer and cybercrimes; and the lack of official records of complaints about digital violence.

Besides, there are **no internationally agreed indicators** that capture the majority of forms of TF VAW or that have been validated in different countries.[282] Moreover, if only measuring one or two forms of TFVAW, prevalence is likely to be underestimated. Measuring the frequency or number of incidents of TFVAW may also be difficult as these may not be distinct. For example, it is unclear whether the initial non-consensual uploading of a sexual image of a

The lack of common indicators for statistical purposes is also a major problem, to which EIGE is responding.

person should be considered a separate incident to the subsequent viewing, distribution and/or storage of the image by others. Moreover, some behaviours, such as the non-consensual distribution of sexual images, only need to occur once to have damaging impacts. Other behaviours, such as sending a message to an intimate partner to ask about their location, may need to occur repeatedly or with other acts to constitute abuse. Frequency measures, thus, need to be tailored to the form of CVAW and account for severity.

Furthermore, **most available data on CVAW**, at international level, **lacks disaggregation by age, sex or other important socio-demographic factors**, thus limiting possibilities for understanding the disproportionate impacts on women, as well as an intersectional analysis of the trends.[283]

6. UNDER-REPRESENTATION OF WOMEN IN TECHNOLOGY

Another key challenge is the significant under-representation of women in science, technology, engineering and mathematics (STEM) professions, and in technology in particular.[284] The absence of women's voices and perspectives affects the extent to which technology is gender responsive. **The embedding of inequalities and systematic biases into ICT technologies is evident in the deficiencies in algorithms**, which promote online VAW and content moderation algorithms, which fail to detect VAW.

As highlighted by the consulted stakeholders,[285] technology is developed by white Western men for men users; the **under-representation of women, including women from ethnic minorities, contributes to the lack of a gender dimension into ICT products** including online gaming and virtual reality platforms, where CVAW is increasing.

7. INADEQUATE SERVICE RESPONSES

There is little awareness of CVAW and its different manifestations among relevant actors including judges, prosecutors, police, health professionals and educators, who lack sufficient training and specialist expertise.[286]

This, in turn, affects women's confidence in service providers and contributes to the under-reporting of CVAW (survivors feel that nothing concrete will be done to support them and, thus, do not report incidents). In addition, technology tools to ensure the collection of evidence are not always available to law enforcement officials. Cyberviolence may involve methods that are particularly difficult for police forces to investigate. Investigation may become even more difficult when offline and online violence are intertwined.[287]

Law enforcement agents and other professionals working with victims **are not adequately equipped with the skills and knowledge** to address cases of online and technology-facilitated violence. As noted in GREVIO's first General Recommendation, such lack of awareness and training can lead to victim blaming and the dismissal of cases.[288] The consequence of this lack of expertise is also the lack of assessment of risk before the escalation of CVAW.[289]

Moreover, there are only a few **specialist support services for women victims of violence in digital spaces**. As highlighted by GREVIO,[290] there is a need for specialist support with the digital dimension of violence against women and girls. For example, there is a need for direct assistance to get content removed, such as non-consensual intimate imagery, and for dealing with online attacks. Specialist guidance is also essential for victims regarding the technology used to facilitate violence against women, such as stalkerware and spyware apps. In this regard, GREVIO noted that there are **few dedicated support services** that comprehensively address the complex issues involved.[291]

Furthermore, like any other form of VAW, CVAW **is often overlooked because of a lack of awareness and understanding of violence among professionals**. Victims' experiences are often considered as isolated incidents rather than patterns of behaviour, and victims are blamed for the violence they face.[292] Victims may also encounter professionals who are unacquainted with the phenomenon and do not understand its potential gravity.[293] They **do not recognise the gendered nature of CV and the continuum of violence between the online and offline words**.

In this regard, for example, victims of cyber violence in Denmark complained about the attitude of the police and reported feelings of not being heard or protected.[294] They described how the police asked them to gather evidence themselves instead of conducting their own

investigation. This is in many ways problematic, and one survivor in Denmark described it as 'being in hell again'. Interviews with representatives of the police in Denmark show that cyber violence is not taken as seriously as other crimes.[295] The lack of emphasis being placed on cases of cyber violence and harassment is not unique to Denmark, as is indicated by other research.[296]

Besides, **survivors' perspectives are often not incorporated in service provision**.[297] Decisions are often made excluding survivors' valuable voices and experiences. Another issue is the insufficient or inadequate **multi-stakeholder cooperation and/or coordination among different service providers**.[298] This results in overlaps of actions and gaps that compromise the effectiveness of responses.

Furthermore, as mentioned by the consulted stakeholders, **actions to tackle CVAW tend to focus on punishment rather than prevention**. The need to change negative attitudes towards women and their role in society in order to prevent online violence and, thus, the need to promote awareness-raising, education and training as means to prevent such violence, have been emphasised by the EDVAW.[299]

Similar problematics also apply to **image-based abuse**. As highlighted in the 2023 report by the Reclaim Coalition,[300] perpetrators of image-based abuse rarely face criminal charges. There are many factors leading to this result, including: **inconsistent enforcement of laws and insufficient specialised, trauma-informed training for law enforcement**. In many countries, this results in legal systems that are incapable of arresting and prosecuting abusers, or, in fact, even identifying and protecting the victims of image-based sexual abuse. Overall, there is a limited capacity of criminal justice systems to prevent or reduce harms.[301]

Another issue, applying to both VAW and CVAW, is the **lack or insufficient funding and/or resources available to victims support services** in order to enable them to effectively support women, as emphasised by GREVIO and EPRS. **Inadequate victim support** amplifies the scope and intensity of CVAW, jeopardising women's participation in online spaces and hindering their ability to fully reap the benefits of the digital age.[302]

8. INEFFECTIVE RESPONSES BY SOCIAL MEDIA AND ONLINE PLATFORMS

Furthermore, **social media and online platforms do not always act effectively to remove illegal and harmful content**. For example, in late January 2024, sexually explicit AI-generated 'deepfake' images of American musician Taylor Swift were proliferated on social media platforms 4chan and X (formerly Twitter). Several artificial images of Swift of a sexual or violent nature were quickly spread among users including youth, with one post reported to have been seen over 47 million times before its eventual removal.[303] Besides, the entire Western Balkan region was shaken in August 2023 when a man livestreamed the torture and murder of his wife on Instagram; the video and the perpetrator's account were removed three hours after the video was posted. During these three hours he killed three persons and wounded another three persons. At one point in time, 15,000 people were watching the livestream. These incidents reveal substantial weaknesses in mechanisms of reporting and removing harmful content, including filters designed to automatically flag and remove violent content.[304]

In general, **social media and online platforms are not always regarded as effective in removing illegal content by users**, despite the EU legislation imposing such obligations (see Section 3.2). According to a survey by HateAid, 80% of respondents think that online platforms are not doing enough to protect people from digital violence. They would like to be able to better control the platforms' algorithm so that they can decide which system is used to show posts. 92% argue in full or in part that illegal content should be removed from the platforms. Likewise, a survey by UN Women found that a high proportion of all women (70.4%) would like stronger accountability and responsibility from companies that own internet platforms and apps and more effective protection from institutions

(66.5%). Among women who reported an incident of TFVAW to the online platform (465 women), action was taken by platforms only in 23.7% of cases (110 women), other official action was taken in 3.5% of cases (24 women), but in 14% of cases (65 women), the representatives of the platform advised women to ignore the incident. [305]

The 2023 FRA report[306] highlights that **a large amount of misogyny and racism slips through content moderation systems designed to prevent it**. Human content checkers can miss online hate. Also, algorithms are prone to errors; they may multiply errors over time, and may even end up promoting online hate. Moreover, exploring content moderation practices within platforms remains even more difficult, as relevant information is very difficult to access. Platforms remain protective when it comes to providing access to their data for a variety of reasons, which may include the protection of business models, privacy concerns and potential fears of revealing flaws in platforms' content moderation practices.

Similar findings come from a 2021 Report on platform liability,[307] according to which when it comes to addressing CVAW, **platform content moderation measures have been deficient in both design and application**. Human reviewers tend to be underpaid third-party contractors working in traumatising conditions who have only seconds to determine whether a given post should be left up, taken down, or escalated. Automated content moderation is rife with further errors, which have resulted in the removal of content, including posts that constitute parody and satire; innocuous images mistaken for nudity.

Criticism was also expressed against **porn companies**. According to experts, **victims report significant delays in getting material removed from porn sites or being ignored**.[308] The high incidence of non-consensual sexual material on mainstream pornography sites legitimises and normalises abuse (see Section 2.3). In this regard, the company that operates Pornhub and other adult websites was prosecuted before the federal court of New York for having profited for years from pornographic content that depicted sex trafficking victims. The company was motivated by profit when it 'enriched itself by turning a blind eye to the concerns of victims who communicated to the company that they were deceived and coerced into participating in illicit sexual activity.' [309]

Furthermore, **tech companies and search engines** like Google often turn a blind eye towards CVAW. As argued by Vera-Gray and McGlynn,[310] by typing 'deepfake porn' or 'nudify' into Google, it immediately offers links to websites dedicated to creating pornography from everyday photos. Within minutes, one can upload fully clothed photos of female colleagues, friends and celebrities, including young girls, and get a nude image back. The fact that Google showcases these websites makes them seem legitimate. In practice, search engines are facilitating the abuse and harassment of women and girls.

Moreover, **complaint reporting systems of online platforms are not always user-friendly**, with the result that victims do not know to whom ask support.[311] Online **platforms' policies on CVAW are often vague** and **incomprehensible**; they do not always include a gender dimension.[312]

V. Good practices to tackle CVAW

This section presents an overview of good practices to tackle CVAW effectively within and outside the EU. Practices of different types have been selected and categorised based on their scope and focus.

GOOD PRACTICES TO TACKLE CVAW

Capacity building

In **Slovenia**, seminars and training sessions were organised for law-enforcement officers and judges with the aim of enhancing their capacity to investigate and prosecute the digital dimension of violence against girls and women. A handbook with guidelines on the roles to be played by the law-enforcement agencies and the judiciary in successfully dealing with cases of online and technology-facilitated violence against women and girls was also adopted and distributed to all Slovenian police stations and directorates, prosecutors' offices and courts.[313]

Likewise, a range of Member States[314] have adopted guidelines for professionals aimed to help them with the recognition and tackling of CVAW. While **France** has specific guidelines on sexist cybercrimes, the Netherlands has produced guidelines for criminal prosecution of abuse of sexual images. **Denmark** produced guidelines on digital sex violations.[315] **Portugal** has adopted a comprehensive set of guidelines on gender and citizenship, which includes guidelines on internet security, for all levels of education, from preschool to secondary education.[316]

Involvement of national human rights institutions

National human rights institutions, such as equality bodies, ombudsman institutions, women's rights organisations and human rights NGOs at national level, **also play an important role in combating CVAW**, particularly when their mandate allows them to investigate cases of online hate speech. The role of such national bodies is also significant as concerns raising awareness on the phenomenon and in elaborating standards. For example, in **Belgium**, the Institute for Equality between Women and Men filed a criminal complaint against a social platform for refusing to take down non-consensual intimate images. The Belgian Institute also submitted a complaint on behalf of a female public figure before the Council of Journalists against an online magazine, which had published a sexist article about the woman after she participated in the public debate on #MeToo.[317] In **Denmark**, the Institute for Human Rights has published a number of studies that address hate speech in the public debate online, providing recommendations.[318]

Prevention

Different examples of good practices aimed to prevent CVAW have been selected: the inclusion of a special curriculum on CVAW in schools; a project involving men and boys in eradicating stereotypes and a study empowering young people to counter disinformation and sexual digital forgeries.

In **Slovenia** different ministries have collaborated to introduce a **special curriculum** into schools addressing the social unacceptability of CVAW. A similar course was attended by teachers,

school counsellors, social workers, and other professionals working with children, as well as specific training for law enforcement personnel and the judiciary.[319]

MenABLE[320] is a 24-month project, co-funded by the European Commission and run by partners in **Belgium, Denmark** and **Greece**. The project aims to **prevent CVAW by tackling its root causes** and by promoting prevention strategies primarily, but not exclusively, targeting boys and young men. Educational tools and awareness activities, conducted as part of the project, aim at primary prevention, changing social norms and behaviour, in order to end tolerance of all forms of VAW. The project focuses on early teens (13-15 years) and late teens (16-18 years) through formal and non-formal educational settings by targeting educational professionals including heads of schools, teachers/educators, caregivers, and other professionals working with young people in youth and sports clubs, camps, libraries, and Safer Internet Centres amongst others.

A **study**,[321] funded by the Social Sciences and Humanities Research Council (SSHRC) and Canadian Heritage, unveils how **empowering youth with digital agency** can be a force against the rising tide of disinformation fuelled by 'deepfake' and artificial intelligence technologies. The study focused on how youth perceive the impact of 'deepfakes' on critical issues and their own process of constructing knowledge in digital contexts. The study explored their capacity and willingness to effectively counterbalance disinformation.

In particular, the research brought together Canadian university students, aged 18 to 24, for a series of hands-on workshops, in-depth individual interviews and focus group discussions. Participants created 'deepfakes', gaining a firsthand understanding of easy access to and use of this technology and its potential for misuse. This experiential learning proved invaluable in demystifying how easily 'deepfakes' are generated. Participants initially perceived 'deepfakes' as an uncontrollable and inevitable part of the digital landscape. Through engagement and discussion, they went from being passive digital sexual forgery bystanders to developing a deeper realization of their grave threat. Critically, they also developed a sense of responsibility in preventing and mitigating sexual digital forgeries' spread, and a readiness to counter sexual digital forgeries.

Survivors' involvement

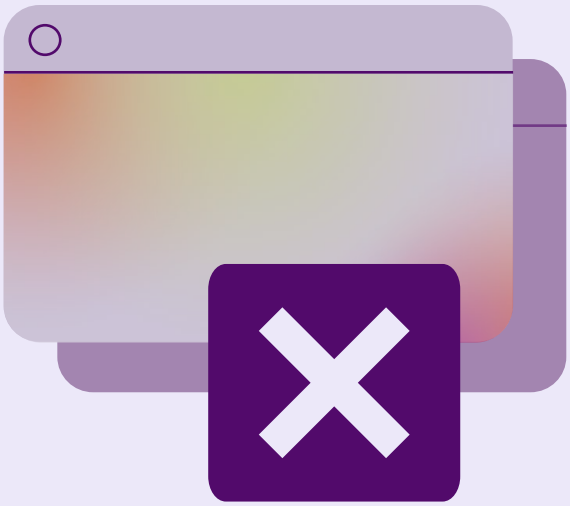
The **Reclaim Coalition to End Online Image-based Sexual Violence**[322] brings together a global network of leaders to accelerate the global response to online image-based sexual violence through shared initiatives across advocacy, policy, technology, and survivor services. The Coalition refers to individuals with firsthand knowledge of image-based sexual violence as 'lived experience experts.' The Coalition gives voice to survivors and their experiences. It works to: facilitate the meaningful exchange of knowledge among coalition members; elevate the issue among key decision makers; amplify advocacy for survivor-informed laws, policies, and accountability standards; support increased

opportunities for lived experience leadership to uplift their expertise, insights, and past experiences.

Helplines

Access Now Digital Security Helpline helps women at risk of violence to improve their digital safety practices and provides emergency assistance for women under attack. The 24/7 Digital Security Helpline offers real-time, direct technical assistance and advice to civil society groups and activists, media organizations, journalists and bloggers, and human rights defenders. They help people and communities at risk to improve digital security practices and provide rapid-response emergency assistance in nine languages.

In Ireland, the online reporting service **Hotline.ie** is available, allowing victims to report the non-consensual sharing of intimate images and videos and take down, where warranted, illegal content.



Countering cyber-sexism and online hate speech

#StopFisha[323] is a French feminist NGO which aims to fight against cyber-sexism. Created in April 2020 during the covid-19 pandemic, the hashtag #StopFisha was created as a counter-movement to the explosion of the dissemination of intimate content without consent. 'Fisha' meaning 'to display' and humiliate, is the name given to the practice of disseminating intimate content. The #StopFisha was therefore created as a support for the victims and as an alert to denounce cyber-sexism. As the movement continued on growing, #StopFisha became an NGO which now fights against all forms of sexist and sexual cyberviolence. The NGO has four main goals: to investigate dangerous accounts and supply detailed information to the police and justice system; to support victims and provide legal assistance to them; to raise awareness around cyber harassment through schools and the media; and to advocate change with policy makers.

'I am here'[324] is a network with more than 150,000 members in 14 countries, which promotes, defends and upholds freedom of speech and democracy. The network supports and empowers the targeted and victimised, acting to counter hate speech and misinformation online. The network has two main activities: to raise awareness on CVAW and to support women who face it.

The #StopFisha was therefore created as a support for the victims and as an alert to denounce cyber-sexism

Specialised support services (outside and within the EU)

In several countries, **specialist law enforcement units** with in-depth knowledge of CVAW are being introduced to ensure effective and responsive police investigations and victim support. Specialist law enforcement units are increasingly common in Latin America. For example, the Federal Police of Mexico has a forensic division responsible for the investigation of cybercrimes, including online and CVAW and girls. Likewise, the National Police of Colombia has a similar Police Centre for Cybernetics, and the Federal Police in Brazil includes an Office for the Suppression of Cybercrime.[325] In Europe, Romania has adopted a national strategy for preventing and combating sexual violence, which set up similar specialist units, both in the law enforcement agency and in the State Prosecutor's Office.

Removal of harmful content

The **UK Revenge Porn Helpline** (RPH) helps prevent individuals from becoming victims of non-consensual intimate image abuse. Since its creation, the RPH has supported thousands of victims, with an over 90% removal rate, successfully removing over 200,000 individual non-consensual intimate images from the internet. More recently, RPH has partnered with Meta to launch **StopNCII.org**, a free tool using innovative technology to support victims of non-consensual intimate image abuse by creating a digital fingerprint of an image that can then be proactively detected and removed by participating platforms and tech companies to prevent the sharing of specific images.[326]

VI. Recommendations

The following recommendations have been formulated based on in-depth desk research, review of legal and policy documents and stakeholder consultation. While the general recommendations apply to all stakeholders in the area of CVAW, specific recommendations have been drafted for the EU institutions and Member States.

1. GENERAL RECOMMENDATIONS

Empower survivors:

As highlighted in Section 4.7 (inadequate service provision), survivors' views and experiences are often ignored in the design, planning and delivering of support services. Listening to the perspectives of female survivors is essential as well as include them in the development and implementation of programmes, policies and service delivery on CVAW. Their perspectives and experiences should be fully integrated in support services and policy making in order to ensure that their needs are adequately met. Survivors often experience victims blaming whereas it is not women's responsibility to prevent CV. A holistic approach that involves legal tools to protect victims and prevent CV and calls on big tech to act on their responsibilities, as well as a coordinated response to challenge sexism and cultural norms to avoid victim blaming is needed.

Enhance women's participation in the technology sector:

The under-representation of women in technology is a major issue contributing to the reinforcing of gender stereotypes, which are drivers of CVAW (see Section 4.6). It is, thus, essential to ensure women's participation in the design of gender-responsive products. This includes the design of technology where women are not sexualised and where safe and accessible reporting mechanisms as well as access to support are easily available. To this end, mandatory quotas for women in ICT companies and measures to increase the representation of women on boards of such companies, could be introduced in line with Directive (EU) 2022/2381[327] on improving the gender balance among directors of listed companies and related measures, as well as scholarships for girls in the area of STEM.

Strengthen multi-stakeholder cooperation:

Reinforce cooperation between a broad range of stakeholders (EU actors, Member States, the technology sector, civil society, survivors of CVAW, national human rights institutions, women's rights organisations etc.) to effectively address online/digital VAW through key partnerships and coordinated actions (e.g. awareness raising campaigns), would avoid the current overlaps and gaps in actions (see Section 4.7).

Exchanges of knowledge among key actors are essential, including learning from countries with more advanced systems for addressing CVAW. To this end, working groups among different types of stakeholders, including tech companies, should be regularly held at EU and national level. All these initiatives should be led by the EU institutions and Member States, rather than be left to the goodwill of individual associations.

Research shows that upholding the responsibilities of online platforms to protect users are one of the solutions to tackle CVAW.

Ensure that the technology sector, in particular social media and online platforms, meet their obligations:

(See also recommendations for EU and Member States in this regard)

Social media and online platforms must be held accountable in the fight against CVAW. These platforms are not merely passive players, they actively shape our lives, influence societal norms, and profit from user engagement even when it involves abuse and CVAW. By allowing harmful and/or illegal content to proliferate unchecked, they evade responsibility and contribute to a toxic online environment. It is imperative that they implement stricter policies aimed to promptly detect and remove harmful/illegal material, enforce them consistently, and invest in technologies and support systems that protect women and users from all forms of abuse, including guaranteeing safety in the design and functioning of their services.

In particular, as explained in Section 4.8, social media companies including social platforms do not always ensure a prompt removal of illegal/harmful content. Research shows that upholding the responsibilities of online platforms to protect users are one of the solutions to tackle CVAW. [328] Thus, the technology sector should proactively, promptly and effectively monitor and remove gender hate speech, sexist and misogynistic content and other forms of CVAW. It should also enhance cooperation with law enforcement to adequately address cases of CVAW and more rapidly lock or remove offenders' accounts. Moreover, they should provide effective resources for users to recognize and intervene against online abuse; to this end, reporting mechanisms/forms should be user-friendly and the contact details of victims' support services and police should be given in their websites.

There is also a need for measures that are not limited to the removal of content but that proactively identify the potential harm that their content and distribution systems can cause to women and marginalised groups (preventive approach), who otherwise continue to bear the burden of protecting themselves from risks. To this end, it is necessary to include the perspective of survivors.

Moreover, social media and platforms should establish and enforce gender-sensitive policies, clearly defining which forms of CVAW are prohibited. In order to be effective, content

management should include a combination of both AI-driven content flagging and human review to remove harmful content. In this regard, human moderators should receive adequate training on how to detect cases of CVAW and relevant applicable legislation. Greater transparency from platform companies on data related to incidents of CVAW, their content moderation policies and decisions, as well as their outcomes is also recommended.

In conclusion, increased transparency and accountability, faster removal, and prevention measures are needed from tech companies,[329] online platforms and social media, including porn companies. To this end, the engagement of such companies is vital.

Approach pornography in the continuum of VAW

The EWL denounces the business of pornography and wants to bring to light the enormous financial profits made by pornography industries, in complicity with prostitution businesses (for which pornography is a very efficient advertising system).[330] The EWL advocates for the EU and Member States to take action to ensure that pornography is recognised as a form of VAW. The public opinion should conceptualize this debate correctly, associating pornography with violence and not with sex.

Member States should take all measures to abolish pornography as a way to protect women's human rights. As shown in the report conducted by LEM Spain,[331] pornography constantly involves different practices that are in fact sexual VAW; this fosters the perpetration of a misogynistic culture that promotes forms of sexual VAW as acceptable sexual practices. Pornography endangers all women because they are women.

2. RECOMMENDATIONS FOR THE EU INSTITUTIONS

The following recommendations are addressed to the EU institutions:

Harmonise definitions and categories of CVAW at EU level and across EU Institutions:

In order to address existing discrepancies across national legal systems that hamper effective protection and prosecution and impact negatively on data collection (see Sections 4.2, 4.3 and 4.5). To date, the only attempt to harmonise legal and statistical definitions of CVAW has been carried out by EIGE.[332] EIGE's definitions should be adopted by all EU institutions. According to it, harmonised definitions of CVAW should incorporate gender and intersectional aspects and recognise the continuum of violence between the offline and online worlds.

However, homogenous gender-sensitive definitions and categories of CVAW are needed not only for stakeholders in the legal and statistical area but for all professionals working on CVAW (policy makers, educators, social workers, NGOs, researchers etc.)[333] so that a common language and approach towards CVAW is taken by all key players.

Develop guidelines and indicators for data collection on CVAW:

in order to address the challenges outlined in Section 4.5 related to the measurement of CV, the EU should develop clear guidelines and indicators supporting Member States in their efforts to collect data on CVAW.

EIGE is currently working in this area; indicators are expected to be published soon. As recommended by EIGE,[334] data should be disaggregated by sex and age of both the victim and the perpetrator and their relationship, as well as the type of CV experienced.

Improve the Directive on VAW and DV in the future and extend its scope:

Overall, the Directive can be considered a valuable instrument in protecting women from the main forms of CVAW. However, some improvements should be made in the context of future updates of the Directive. Considering the links between CV and rape (see Section 3.2), rape as sex without freely given consent should be included in the text. References to the intentionality of the conducts and to serious harm should be eliminated as they impose an onerous burden of proof on the victim.

Concerning Article 5, the freedom of expression and arts considerably limits the scope of this provision, thus, they should be deleted or better balanced with the privacy of the person whose images are shared without consent. As recommended by experts,[335] the restriction of scope to only material of people 'engaging in sexual activity' in Article 5(b) should be removed, utilising the broader definition of 'intimate images'. Similarly, in relation to threats (Article 5 (c)), the limitation of this provision to only cases where it can be proven the threat was designed to coerce the individual into specific acts or omissions should be deleted. A threat to distribute such material, without consent, is harmful, regardless of the motives.[336]

The exception of Article 8 (on incitement to hatred or violence), according to which, Member States may choose to punish only the conduct which is likely to disturb public order or which is threatening, abusive or insulting, should be removed as it leaves the punishment of the behaviour to the discretion of judicial authorities.

According to the EWL, the production and dissemination of pornographic material depicting acts of sexual violence should be included in the review of the Directive as it is a form of sexual exploitation. The scope of the crime should be extended to cover all forms of image based sexual abuse, including pornography.

Update existing EU legislation to tackle the gender nature of CV:

The Victim Rights Directive should be updated with the aim to incorporate articles specifically dedicated to CV and its gender dimension.[337] As mentioned in Section 3.2, the rights and needs of victims of CV may differ from the rights and needs of victims in general, in particular their need for specialised support services should be taken into account given the complexity and heterogeneous nature of CV.

The 2008 Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law should also be updated to incorporate reference to gender hate speech by ICT means. Given the sharp rise in hate speech and hatred against women,[338] the consulted stakeholders[339] agreed on the need to regulate it.

To date, many social media and online platforms are not meeting their obligations under the DSA as often they do not take prompt action to remove illegal content

Effectively enforce the DSA:

As mentioned in Section 3.2, the European Commission has enforcement and investigative powers in relation to the obligations under the DSA. It is paramount that the Commission effectively exercise these powers (including the imposition of fines), in cooperation with National Digital Service Coordinators, in order to guarantee that online platforms and intermediary services meet their obligations in line with the DSA. The enforcement of Articles 34 and 35, which refer to GBV, are of particular importance. To date, many social media and online platforms are not meeting their obligations under the DSA as often they do not take prompt action to remove illegal content (see Section 4.8). It is also important that other porn platforms are designated by the Commission as VLOPs, as it happened for Pornhub, XVideos and Stripchat in December 2023.

Incorporate reference to CVAW under the Artificial Intelligence Act:

Evidence shows an increased use of AI to commit CVAW and a rapid evolution of AI technologies to perpetrate gender discrimination, which is one of the root causes of CV (see Section 2.3). In light of the proliferation of sexual digital forgeries (known as 'deepfakes') and other forms of VAW through AI, it is recommended that future updates of the AI Act address CV through a comprehensive gender-sensitive approach. It is also important that specific mention of CVAW is included among 'high risks' (beyond reference to gender equality in Recital 28(a)) thus, providers will be obliged to carry out risk assessments.

Issue regular guidance on new forms of CVAW:

Given the rise in forms of CVAW facilitated by artificial intelligence (see Section 2.3) and the incapacity of legal/policy frameworks to keep at pace with new ICT developments (Section 4.4.), the EU should issue a guidance on how to tackle the latest forms of CVAW in an effective way. This could take the form of guidelines regularly updated based on latest ICT developments.

3. RECOMMENDATIONS FOR MEMBER STATES

Align national definitions of CVAW with harmonised gender-sensitive EU definitions:

To tackle the challenges outlined in Section 4.2 and 4.3 (lack of harmonised definitions and discrepancies among legal & policy frameworks), Member States should incorporate EU harmonised definitions and categories of CVAW, into their own legal and policy frameworks as well as in their statistical/data collection systems to ensure the collection of comparable data across countries. In 2022, EIGE issued definitions on CVAW at EU level. Definitions of four forms of CV are now contained in the Directive on VAW.

Collect quality data on CVAW in a regular manner:

In line with Article 11 of the Istanbul Convention and Article 44 of the Directive on VAW, Member States should collect data on CVAW of good quality, which are comparable and disaggregated, following EIGE's guidelines.

Data collection should take place regularly and should cover both CV as a whole phenomenon as well as its specific forms. Member States should also comply with their obligations to take part in EU surveys.

Ratify and implement the Istanbul Convention:

The Istanbul Convention was signed on behalf of the EU on 13 June 2017, triggering the entry into force on 1 October 2023. However, to date six Member States (BG, CZ, HU, LV, LT and SK) have not ratified the Convention. The Convention is a key instrument to protect all women from all forms of violence including CVAW, therefore, it is important that it is fully implemented by all Member States. Moreover, in line with GREVIO Recommendation n.1, Member States should ensure recognition of the digital dimension of VAW in national strategies, programmes and action plans on VAW as part of a holistic response to all forms of violence, as required by Article 7 of the Istanbul Convention.

Strengthen prevention in the broad sense:

As highlighted in Sections 4.1, 4.6 and 4.7, there is a lack of understanding of CVAW among service providers as well as the tendency to blame victims for incidents. It is paramount to transform gender stereotypes and social norms at the broader societal level including through the empowerment of women. As part of their prevention strategies, Member States should raise awareness among all professionals about the manifestations and consequences of CVAW.

Prevention and awareness of CVAW should also be integrated into school education programs from an early age for both boys and girls.[340] This would require mainstreaming gender equality and awareness of offline and online violence in national curricula and teaching/learning materials for the entire education cycle (from primary to tertiary education). Programs on digital literacy and safety online would not be enough to guarantee that the root causes of CVAW are eradicated.[341]

Moreover, as recommended by the EWL in its report,[342] implement mandatory, relationship and sexuality education from a feminist perspective is paramount. Feminist sexuality education should be mainstreamed across subjects in the school curricula drafted by the Ministry of Education or other relevant authorities. The competent authorities should make sure that higher education courses for primary teachers are accredited only if they provide adequate training for sexuality education as a compulsory part of their curriculum. The quality of this curriculum should be monitored by national women's rights organisations, and the European Association for Quality Assurance in Higher Education (ENQA). Member States must also ensure resourcing is committed to ensure robust provision of feminist sexuality education.

Feminist sexuality education can address the sexist power-relations in both sexuality and pornography in a truly critical and structural manner. Such education emphasises the right to engage in or refuse to engage in sexual acts without coercion, fear of violence, stigmatisation and discrimination, and empowers youth to exercise this right. It helps young people to be critical about pornography and the fetishisation of violence in popular culture. Given the wide-reaching, powerful and harmful influence of online pornography, and its inherently cross-border nature, Member States should impose unified and stringent regulations on its content and accessibility, within and beyond the education sector.

Educating men and boys on the forms, severity and consequences of CVAW is also crucial. The focus should be on the forms of CV that may already be normalised or are at risk of being normalised, as well as more generally on equitable masculinities and non-violent communication. More generally, men and boys should be involved in prevention initiatives aiming to eradicate gender stereotypes both online as much as offline.

Overall, a cultural systematic change is required to tackle CVAW from a gender and an intersectional perspective and as a continuum of violence. Changing social attitudes and norms is necessary to shifting the way online/digital abuse is understood and avoid victim-blaming.[343]

Criminalise CVAW in line with the Directive on VAW:

At national level, CVAW is often covered by general offences rather than specific offences (see Section 3.3). Moreover, national legislation is often outdated as unable to keep pace with ICT developments. It is recommended that Member States criminalise the main forms of CVAW in line with Articles 5 to 8 of the new Directive on VAW

and keep the legislation abreast of technology developments. As outlined above, the Directive on VAW is not as ambitious as it could have been and there are still improvements to be made in order to make the legislation more effective. Member States during the transposition phase should go beyond the minimum standards of protection set by the Directive.

Effectively monitor and enforce compliance with the DSA:

As explained in Section 3.2, Member States play a vital role in enforcing the DSA's obligations. National Digital Service Coordinators (DSCs) have extensive investigative and enforcement powers, including making compliance agreements, imposing interim measures, fines and penalties. Given that the responses towards cases of CVAW by online platforms and social media are often inadequate, it is essential that National DSCs effectively monitor and enforce compliance with the DSA. This includes the imposition of fines and, in particularly serious cases, the restriction of the users' access to the service. However, since national interpretation and enforcement of the DSA will be influenced to a large extent by judicial decisions, it is paramount that judicial authorities receive adequate training on the DSA' obligations with regards to CVAW (see section below on specialist support services).

Ensure accountability:

Laws and policies of Member States should ensure the responsibility of perpetrators and the accountability of the technology sector, including in the case of transborder acts of CV. The effective enforcement of the legal framework on CVAW is crucial. As pointed out by the consulted stakeholders, cases of CVAW rarely end up before courts and often lead only to light sentences.[344] As highlighted by CoE,[345] it is essential to regularly train law enforcement professionals to be able to effectively investigate and prosecute CV from a gender perspective and as a continuum of violence. In this context, guidelines for police, prosecutors and judges on how to deal with cases of CVAW (avoiding victim-blaming), should be adopted at national level.

Improve victims' access to remedies:

As highlighted in Section 4.7, victims do not always know to whom they should report the abuse. Complaint report systems are not always user friendly (see general recommendations). It is, thus, important to guarantee easily accessible and safe reporting mechanisms both online and offline, enabling women to report CV. Information on legal avenues and other remedies should be made easily accessible to victims of CVAW.

Provide ad-hoc specialised support services:

Poor and/or inadequate service provision is a major issue affecting victims of CVAW (see Section 4.7). It is, therefore, essential to strengthen capacities of service providers from different sectors to respond to the unique nature of CVAW and the needs of survivors. Specialised survivor-centred support, with ICT expertise, should be ensured through adequate funding and resources. Provide mandatory and continuous education and training for all relevant professionals (judges, prosecutors, police, social workers, educators etc.), to equip them with knowledge on digital expressions of VAW, would enable them to respond to women without causing secondary victimisation and re-traumatisation.

Annex I
References

ANNEX I REFERENCES

Almenar, R. (2021). Cyberviolence against women and girls: Gender-based violence in the digital age and future challenges as a consequence of Covid-19. Trento Student Law Review, 3(1), 167-230.

Bailey, L., Hulley, J., Gomersall, T., Kirkman, G., Gibbs, G., & Jones, A. D. (2024). The Networking of Abuse: Intimate Partner Violence and the Use of Social Technologies. Criminal Justice and Behavior, 51(2), 266-285.

Barker, K., & Jurasz, O. (2024). Digital and online violence: international perspectives. International Review of Law, Computers & Technology, 38(2), 115-118.

CIPESA (2020), In Search of Safe Spaces Online: Research Summary. https://cipesa.org/wp-content/files/publications/WomenAtWebUg_In-search-of-safe-spaces-online.pdf

Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform. https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae

De Vido, S. and Sosa, L. (2021), Criminalisation of gender-based violence against women in European states, including ICT-facilitated violence. Publications Office of the European Union, Luxembourg. https://op.europa.eu/en/publication-detail/-/publication/25712c44-4da1-11ec-91ac-01aa75ed71a1

European Commission (2022), Study on online identity theft and identity-related crime. Final report. https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1/language-en

European Commission (2020), Advisory Committee on Equal Opportunities for Women and Men (2020), Opinion on combatting online violence against women. Brussels. https://ec.europa.eu/info/sites/default/files/aid_%20development_cooperation_fundamental_rights/%20opinion_online_violence_against_women_2020_%20en.pdf

European Union Agency for Fundamental Rights (FRA) (2014), Violence against Women: An EU-wide survey – Main results report. Publications Office of the European Union, Luxembourg https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

European Union Agency for Fundamental Rights (FRA) (2017), Challenges to Women's Human Rights in the EU – Gender discrimination, sexist hate speech and gender-based violence against women and girls. Publications Office of the European Union, Luxembourg https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-challenges-to-women-human-rights_en.pdf

European Union Agency for Fundamental Rights (FRA), (2023), Online Content Moderation Current Challenges In Detecting Hate Speech. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-online-content-moderation_en.pdf

European Institute for Gender Equality (EIGE) (2022), Combating cyber violence against women and girls. Vilnius. https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls?language_content_entity=en

European Institute for Gender Equality (EIGE) (2021), Artificial intelligence, platform work and gender equality. https://eige.europa.eu/publications-resources/publications/artificial-intelligence-platform-work-and-gender-equality?language_content_entity=en

European Institute for Gender Equality (EIGE) (2017), Cyber violence against women and girls. Vilnius. https://eige.europa.eu/publications/cyber-violence-against-women-and-girls

Europol (2020), The challenges of countering human trafficking in the digital era. https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf

Europol (2020), Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. https://www.europol.europa.eu/publications-events/publications/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic

European Women's Lobby (EWL), (2017), #HerNetHerRights, Mapping the state of online violence against women and girls in Europe. https://www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf

European Parliament Research Service (EPRS), (2021), Combating Gender based Violence: Cyber Violence. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621

European Parliament Research Service (EPRS) (2021), Tackling deepfakes in European policy. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

European Liberal Forum (2021), Violence Against Women In European Politics.

Equality Now (2023), Briefing Paper: Deepfake Image-Based Sexual Abuse, Tech-Facilitated Sexual Exploitation And The Law.

Equality Now (2021), Ending Online Sexual Exploitation and Abuse of Women and Girls.

eSafety Commissioner Australia (2021), For My Safety': Experiences of Technology-Facilitated Abuse among Women with Intellectual Disability or Cognitive Disability.

Fraser, C., Olsen, E., Lee, K., Southworth, C., & Tucker, S. (2010). The new age of stalking: Technological implications for stalking. Juvenile and family court journal, 61(4), 39-55.

Flynn, A., Powell, A., & Hindes, S. (2021). Technology-facilitated abuse: A survey of support services stakeholders.

GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence. Learning Brief 1: Understanding technology-facilitated GBV.

Glitch, U. K., & Coalition, E. V. A. W. (2020). The ripple effect: COVID-19 and the epidemic of online abuse. no. September, 48.

Gray, K. L., Buyukozturk, B., & Hill, Z. G. (2017). Blurring the boundaries: Using Gamergate to examine 'real' and symbolic violence against women in contemporary gaming culture. Sociology compass, 11(3), e12458.

Gurumurthy, A., Vasudevan, A., & Chami, N. (2019). Born digital, born free? A socio-legal study on young women's experiences of online violence in South India. A Socio-Legal Study on Young Women's Experiences of Online Violence in South India (August 1, 2019).

Layden, M. A. (2010). Pornography and violence: A new look at the research. The social costs of pornography: A collection of papers, 57-68.

Utah Domestic Violence Coalition, 2009, available at: www.udvc.org. Silbert & Pines, 1984: In her research with 200 women in prostitution, Mimi Silbert recognised the role played by pornography in legitimising victimisation; in the account of rape, almost a quarter of these women made reference to pornography used by the rapist.

HateAid (2021), Boundless hate on the internet – Dramatic situation across Europe. https://hateaid.org/wp-content/uploads/2022/04/HateAid-Report-2021_EN.pdf

Taibat Hussain, Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery, Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, Adrian J. Scott, The British Journal of Social Work, Volume 54, Issue 4, June 2024, Pages 1777–1779, https://academic.oup.com/bjsw/article-abstract/54/4/1777/7588791?redirectedFrom=fulltext

Hicks, J. (2021), Global evidence on the prevalence and impact of online gender-based violence (OGBV).

Iyer, N. et Al. (2020), Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet. APC and IDRC.

Inter-Parliamentary Union (2021), Sexism, Harassment and Violence against Women in Parliaments in Africa.

Jagayat, A., & Choma, B. L. (2021). Cyber-aggression towards women: Measurement and psychological predictors in gaming communities. Computers in human behavior, 120, 106753.

Jenson J., De Castell S. (2021). Patriarchy in play: Video games as gendered media ecologies. Explorations in Media Ecology, 20(2), 195–212. https://doi.org/10.1386/eme_00084_1

Khoo, C. (2021). Deplatforming misogyny: Report on platform liability for technology-facilitated gender-based violence. Report, LEAF, Toronto.

Leonard D. J. (2019). Virtual anti-racism: Pleasure, catharsis, and hope in Mafia III and Watch Dogs 2. Humanity and Society, 44(1), 111–130. https://doi.org/10.1177/0160597619835863

Macêdo Callou, R.C. et al. (2021), Cyberbullying and gender violence in online games. https://www.researchgate.net/publication/352330454_Cyberbullying_and_gender_violence_in_online_games

McGlynn, C., Johnson, K., Rackley, E., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2021). 'It's torture for the soul': The harms of image-based sexual abuse. Social & legal studies, 30(4), 541-562.

National Democratic Institute (2019), 'Tweets That Chill: Analyzing Online Violence Against Women in Politics'.

Naffi, N. et Al. (2023) Empowering Youth to Combat Malicious Deepfakes and Disinformation: An Experiential and Reflective Learning Experience Informed by Personal Construct Theory, Journal of Constructivist Psychology. https://www.tandfonline.com/doi/full/10.1080/10720537.2023.2294314

Panorama Global, (2023) I DIDN'T CONSENT: A Global Landscape Report on Image-Based Sexual Abuse, Prepared by: The Image-Based Sexual Abuse Initiative. https://assets-global.website-files.com/62448c65f2a3dc7ae94193bd/63fe26f284d41703fac49b17_IBSA%20Landscape%20Report%202023%20by%20Panorama%20Global%20v20230228.pdf

Parsons et Al. (2019), The Predator in Your Pocket. A Multidisciplinary Assessment of the Stalkerware Application Industry, University of Toronto. https://tspace.library.utoronto.ca/bitstream/1807/96320/1/stalkerware-holistic.pdf

Patrini, G. (2019), Mapping the Deepfake Landscape. Sensity (blog). https://sensity.ai/mapping-the-deepfake-landscape/

Patrini, G. (2020) Automating Image Abuse: Deepfake Bots on Telegram. Sensity (blog). https://sensity.ai/automating-image-abuse-deepfake-bots-on-telegram/

Plan International (2020). Free to Be Online? Girls' and young women's experiences of online harassment. Available at: https://plan-international.org/publications/free-to-be-online/

Porta, C. et al. (2024) Sexual Violence in Virtual Reality, A Scoping Review.Journal of Forensic Nursing 20(1):p 66-77, 1/3 2024 https://journals.lww.com/forensicnursing/fulltext/2024/03000/sexual_violence_in_virtual_reality__a_scoping.8.aspx

Posetti, J., et AL. (2021). The chilling: Global trends in online violence against women journalists. UNESCO Research Discussion Paper. https://unesdoc.unesco.org/ark:/48223/pf0000377223/PDF/377223eng.pdf.multi

Rigotti, C. and Al. (2023), Towards an EU criminal law on violence against women: The

ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. Published in: New Journal of European Criminal Law https://cris.vub.be/ws/portalfiles/portal/92354738/20322844221140713.pdf

Rothermel, A.-K. (2023). The role of evidence-based misogyny in antifeminist online communities of the 'manosphere'. Big Data & Society, 10(1). https://doi.org/10.1177/20539517221145671

Singh K. (2022). In the metaverse, sexual assault is very real—So what can we do legally? https://www.refinery29.com

Smith, G., & Rustagi, I. (2021). When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity. Stanford Social Innovation Review. https://doi.org/10.48558/A179-B138

Tang, W. Y., Reer, F., & Quandt, T. (2020). The interplay of gaming disorder, gaming motivations, and the dark triad. Journal of Behavioral Addictions, 9(2), 491–496. https://doi.org/10.1556/2006.2020.00013

The Economist Intelligence Unit (2021), Measuring the Prevalence of Online Violence against Women. A survey was conducted across 45 countries (a sample of 100 replies for each country). https://onlineviolencewomen.eiu.com/

The Nordic Gender Equality Fund (2017), Online violence against women in the Nordic Countries. https://www.nikk.no/wp-content/uploads/Report-Online-Violence-Single-page-Web.pdf

Turillazzi, A. et Al. (2023) The digital services act: an analysis of its ethical, legal, and social implications, Law, Innovation and Technology, 15:1, 83-106. https://www.tandfonline.com/doi/full/10.1080/17579961.2023.2184136

The global partnership, (2023), Technology-Facilitated Gender-Based Violence: Preliminary Landscape Analysis.

The UN Broadband Commission, (2015), Cyber violence against women and girls. https://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf

UN Expert Group (2023), Technology-facilitated Violence against Women: Towards a common definition Report of the meeting of the Expert Group 15-16 November 2022, New York, USA.

UN Human Rights Council (2018), 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, A/HRC/38/47, 18 June.

United Nations (2022), Report of Secretary General, Intensification of efforts to eliminate all forms of violence against women and girls. A/77/302.

United Nations Population Fund (UNFPA), (2023), Measuring technology-facilitated gender-based violence. A discussion paper.

United Nations Population Fund (UNFPA), (2021), Making all spaces safe. New York.

UNESCO (2020), Online violence against women journalists: a global snapshot of incidence and impacts.

UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

UN Women (2023), The State of Evidence and Data Collection on Technology-facilitated Violence against Women.

UN Women, (2023) Technology-facilitated Violence against Women: Taking stock of evidence and data collection.

Van de Heyning C. et al. (2023), Les Deepnudes Parmi Les Jeunes Belges. Bruxelles.

Vera-Gray, F., McGlynn, C., Kureshi, I., & Butterby, K. (2021). Sexual violence as a sexual script in mainstream online pornography. The British Journal of Criminology, 61(5), 1243-1260.

World Wide Web Foundation (2021), Online Gender-Based Violence and Abuse: Consultation Briefing. https://uploads-ssl.webflow.com/61557f76c8a63ae527a819e6/615585a9bbfeb8836d512947_OGBV_ConsultationBriefing.pdf

World Wide Web Foundation and World Association of Girl Guides and Girl Scouts (2020), Survey Young People's Experience of Online Harassment.

World Wide Web Foundation, (2021). Tech Policy Design Lab: Online Gender-Based Violence and Abuse: Outcomes and Recommendations. World Wide Web Foundation.

Wheatcroft, J. et Al. (2017). Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals Coping Responses. SAGE Open.

World Economic Forum (2024), The Global Risk Report 2024. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Wiederhold B.K., (2022). Sexual Harassment in the Metaverse, Brenda K. Wiederhold. https://www.liebertpub.com/doi/full/10.1089/cyber.2022.29253.editorial

Incels: A First Scan of the Phenomenon (in the EU) and its Relevance and Challenges for P/CVE

European Court of Human Rights, (2023). Fact Sheet Hate Speech. https://www.echr.coe.int/documents/d/echr/FS_Hate_speech_ENG

Websites

(Last accessed in August 2024)

Artificial intelligence, deepfakes, and the uncertain future of truth | Brookings. https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/

Toxic Twitter - A Toxic Place for Women - Amnesty International https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1-1/

Deepfakes: How to empower youth to fight the threat of misinformation and disinformation (theconversation.com) https://theconversation.com/deepfakes-how-to-empower-youth-to-fight-the-threat-of-misinformation-and-disinformation-221171

How Technology-Facilitated Gender-Based Violence Impacts Women and Girls (unric.org) https://unric.org/en/how-technology-facilitated-gender-based-violence-impacts-women-and-girls/

The Sustainable Development Agenda - United Nations Sustainable Development https://www.un.org/sustainabledevelopment/development-agenda/

Cyberviolence against women - Cyberviolence (coe.int) https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women

NCII: 90% of victims of are women - Cyber Rights Organization (cyberights.org) https://cyberights.org/ncii-90-of-victims-of-the-distribution-of-non-consensual-intimate-imagery-are-women/

Sexual assault in the metaverse is part of a bigger problem – Monash Lens https://lens.monash.edu/@politics-society/2022/07/22/1384871/sexual-assault-in-the-metaverse-theres-nothing-virtual-about-it

jfn_00_00_2023_10_23_porta_jfn-23-061_sdc2.docx (live.com) https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fcdn-links.lww.com%2Fpermalink%2Fjfn%2Fa%2Fjfn_00_00_2023_10_23_porta_jfn-23-061_sdc2.docx&wdOrigin=BROWSELINK

FRA, Crime, Safety and Victims Rights. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-crime-safety-victims-rights_en.pdf

ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf (hateaid.org) https://hateaid.org/wp-content/uploads/2022/04/ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf

Sealioning' Is A Common Trolling Tactic On Social Media--What Is It? | Berkman Klein Center (harvard.edu) https://cyber.harvard.edu/story/2019-03/sealioning-common-trolling-tactic-social-media-what-it

La nuova Mappa dell'Intolleranza 7- Vox Diritti http://www.voxdiritti.it/la-nuova-mappa-dellintolleranza-7/

Toxic Twitter - Triggers of Violence and Abuse Against Women on Twitter - Amnesty International https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2-3/

The digital dimension of gender-based violence - European Disability Forum (edf-feph.org) https://www.edf-feph.org/blog/the-digital-dimension-of-gender-based-violence/

No space for violence against women and girls in the digital world - Commissioner for Human Rights (coe.int) https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

Violence against women active in politics in the EU (europa.eu) https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/759600/EPRS_BRI(2024)759600_EN.pdf

EWL Observatory Analysis of definitions of rape in the EU- The added value the EU Directive on VAW https://womenlobby.org/EWL-Observatory-Analysis-of-definitions-of-rape-in-the-EU-The-added-value-of?lang=en

What is Zoombombing? Definition from SearchSecurity (techtarget.com) https://www.techtarget.com/searchsecurity/definition/Zoombombing

There's a pandemic of online violence against women and girls - World Wide Web Foundation https://webfoundation.org/2020/07/theres-a-pandemic-of-online-violence-against-women-and-girls/

Crime, Safety and Victims' Rights – Fundamental Rights Survey. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-crime-safety-victims-rights_en.pdf

Bumble - Bumble Backs Law to Ban Cyberflashing in 27 Countries https://bumble.com/en/the-buzz/bumble-backs-law-to-ban-cyberflashing-27-countries-eu-europe

Les Français et le cyberharcèlement Ampleur du phénomène, conséquences, préoccupations et idées reçues (ipsos.com) https://www.ipsos.com/sites/default/files/ct/news/documents/2021-12/Enquete%20Ipsos-Meetic.pdf

Cyberbullying: Twenty Crucial Statistics for 2024 | Security.org https://www.security.org/resources/cyberbullying-facts-statistics/

Ipsos_FéministesCyber_Rapport Volet VICTIMES _V3_08122022.pdf - Google Drive https://drive.google.com/file/d/1uaWxIgLY7p2tc7Rv6DnkCMfOKEDgwxK6/view

Toxic Twitter - A Toxic Place for Women - Amnesty International https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1-1/

The State of Online Harassment | Pew Research Center'. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

Inside the secret world of trading nudes - BBC News https://www.bbc.co.uk/news/uk-62564028.amp

Amnesty reveals alarming impact of online abuse against women - Amnesty International https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women-2/

Commission on Status of Women Concludes 2011 Session with Adoption of Conclusions Aimed at Boosting Women's Access to Education in Science, Technology Fields | Meetings Coverage and Press Releases (un.org) https://press.un.org/en/2011/wom1859.doc.htm

Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders : https://digitallibrary.un.org/record/764453

Transforming our world: the 2030 Agenda for Sustainable Development | Department of Economic and Social Affairs (un.org) https://sdgs.un.org/2030agenda

The right to privacy in the digital age : (un.org) https://digitallibrary.un.org/record/3896430?ln=en

Violence against women: Council and European Parliament reach deal on EU law - Consilium (europa.eu) https://www.consilium.europa.eu/en/press/press-releases/2024/02/06/violence-against-women-council-and-european-parliament-reach-deal-on-eu-law/

Navigating Policy Designs: A Case for Specific and Broad Policies to Counter New Forms of Technology-Facilitated Violence | GenderIT.org https://genderit.org/articles/navigating-policy-designs-case-specific-and-broad-policies-counter-new-forms-technology

EWL Priorities for the Trilogues: Rape must be made an (...) (womenlobby.org) https://www.womenlobby.org/EWL-Priorities-for-the-interinstitutional-negotiations?lang=en

Commission proposes to strengthen the rights of victims of crime https://ec.europa.eu/commission/presscorner/api/files/document/print/%20nl/ip_23_3724/IP_23_3724_EN.pdf

Report: Majority of trafficking victims are women and girls (un.org) https://www.un.org/sustainabledevelopment/blog/2016/12/report-majority-of-trafficking-victims-are-women-and-girls-one-third-children/

Commission designates second set of Very Large Online Platforms under the Digital Services Act | Shaping Europe's digital future (europa.eu) https://digital-strategy.ec.europa.eu/en/news/commission-designates-second-set-very-large-online-platforms-under-digital-services-act

EU Tech Policy Brief: July 2023 - Center for Democracy and Technology (cdt.org) https://cdt.org/insights/eu-tech-policy-brief-july-2023/

A feminist vision for the EU AI Act (fem-ai-center-for-feminist-artificial-intelligence.com) https://www.fem-ai-center-for-feminist-artificial-intelligence.com/_files/ugd/f05f97_0c369b5785d944fea2989190137835a1.pdf

Summary report of the public consultation on fake news and online disinformation | Shaping Europe's digital future (europa.eu) https://digital-strategy.ec.europa.eu/en/library/summary-report-public-consultation-fake-news-and-online-disinformation#:~:text=The%20public%20consultation%20took%20place%20between%2013%20November,actions%20to%20address%20different%20types%20of%20fake%20news.

Final report of the High Level Expert Group on Fake News and Online Disinformation | Shaping Europe's digital future (europa.eu) https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation

TFGBV_Brochure-1000x560.pdf (unfpa.org) https://www.unfpa.org/sites/default/files/resource-pdf/TFGBV_Brochure-1000x560.pdf

No space for violence against women and girls in the digital world - Commissioner for Human Rights (coe.int) https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

Technology is changing faster than regulators can keep up - here's how to close the gap | World Economic Forum (weforum.org) https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/

Challenges to the investigation and prosecution - Cyberviolence (coe.int) https://www.coe.int/en/web/cyberviolence/challenges-to-the-investigation-and-prosecution

Op-Ed: Tackling the hidden perils of technology-facilitated violence against women | UN Women – Europe and Central Asia https://eca.unwomen.org/en/stories/op-ed/2023/11/op-ed-tackling-the-hidden-perils-of-technology-facilitated-violence-against-women

Inside the Taylor Swift deepfake scandal: 'It's men telling a powerful woman to get back in her box' | Deepfake | The Guardian https://www.theguardian.com/technology/2024/jan/31/inside-the-taylor-swift-deepfake-scandal-its-men-telling-a-powerful-woman-to-get-back-in-her-box

Pornhub's Parent Company Admits to Profiting From Sex Trafficking - The New York Times (nytimes.com) https://www.nytimes.com/2023/12/21/nyregion/pornhub-aylo-profits-sex-trafficking.html

Fake Porn, Real Victims: We must stop the easy use of AI to create nude images of women & girls (thejournal.ie) https://www.thejournal.ie/readme/online-safety-spain-artificial-intelligence-6182025-Oct2023/?utm_source=shortlink

Transparency reports: How social media platforms fail on users' rights — HateAid https://hateaid.org/en/transparency-reports-social-media-plattforms/

Plainte au pénal contre Twitter pour la distribution non-consensuelle d'images intimes | Institut pour l'égalité des femmes et des hommes https://igvm-iefh.belgium.be/fr/actualite/plainte_au_penal_contre_twitter_pour_la_distribution_non_consensuelle_dimages_intimes

Homepage - MenABLE
https://www.menable.eu/

Chikane under valgkamp får lokalpolitikere til at trække sig: Partierne må på banen | Institut for Menneskerettigheder https://menneskeret.dk/nyheder/chikane-valgkamp-faar-lokalpolitikere-traekke-partierne-maa-paa-banen

The Reclaim Coalition | Panorama Global
https://www.panoramaglobal.org/reclaim

#StopFisha – INACH
https://www.inach.net/stopfisha/#:~:text=Created%20in%20April%202020%20during%20the%20quarantine%2C%20the,given%20to%20the%20practice%20of%20disseminating%20intimate%20content.

About Us – #IAmHere Movement (iamhereinternational.com)
https://iamhereinternational.com/about-us/

About StopNCII.org | StopNCII.org
https://stopncii.org/about-us/

Legal/policy documents

GREVIO (Expert group on action against violence against women and domestic violence) (2021), General Recommendation No 1 on the digital dimension of violence against women, Council of Europe, Strasbourg, 20 October
https://rm.coe.int/%20grevio-rec-no-on-digital-violence-against-women/1680a49147

Council of Europe (2011), Convention on preventing and combating violence against women and domestic violence.
https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210

ECOSOC Resolution 2003/44, Agreed conclusions of the Commission on the Status of Women on participation in and access of women to the media, and information and communication technologies and their impact on and use as an instrument for the advancement and empowerment of women.
https://www.un.org/en/ecosoc/docs/2003/resolution%202003-44.pdf

United Nations, General recommendation No. 36 (2017) on the right of girls and women to education https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-36-2017-right-girls-and

United Nations, General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992) https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-35-2017-gender-based

United Nations, General recommendation No. 34 (2016) on the rights of rural women.
https://digitallibrary.un.org/record/835897?v=pdf

United Nations, 38th session of the Human Rights Council https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session38/res-dec-stat

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 : note / by the Secretariat https://digitallibrary.un.org/record/1641160?ln=en#record-files-collapse-header

Intensification of efforts to prevent and eliminate all forms of violence against women and girls : resolution / adopted by the General Assembly https://digitallibrary.un.org/record/3896021?ln=en

The right to privacy in the digital age : resolution / adopted by the General Assembly https://digitallibrary.un.org/record/3896430?ln=en

Intensification of efforts to eliminate all forms of violence against women and girls : report of the Secretary-General https://digitallibrary.un.org/record/3988297?ln=en

Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls https://www.unwomen.org/sites/default/files/2023-03/CSW67_Agreed%20Conclusions_Advance%20Unedited%20Version_20%20March%202023.pdf

European Parliament (2020), Report on intellectual property rights for the development of artificial intelligence technologies. https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_EN.html

Council of Europe Convention on preventing and combating violence against women and domestic violence (Instanbul Convention, 2011) https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210

European Parliament (2023), EU accession to the Istanbul Convention https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739323/EPRS_ATA(2023)739323_EN.pdf

Council of Europe (2011), Explanatory report to the Council of Europe Convention on preventing and combating violence against women and domestic violence, Council of Europe Treaty Series, No 210 https://rm.coe.int/%20ic-and-explanatory-report/16808d24c6

The Istanbul Convention: A Missed Opportunity in Mainstreaming Cyberviolence against Women in Human Rights Law? (2022). https://www.ejiltalk.org/the-istanbul-convention-a-missed-opportunity-in-mainstreaming-cyberviolence-against-women-in-human-rights-law/

Council of Europe, Convention 108 and Protocols, Data Protection https://www.coe.int/en/web/data-protection/convention108-and-protocol

CETS 185 (2011), Convention on Cybercrime https://rm.coe.int/1680081561

Council of Europe, Convention on Cybercrime (ETS No. 185) The Budapest Convention and its Protocols https://www.coe.int/en/web/cybercrime/the-budapest-convention

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) (2007) https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201

Council of Europe (2019), Council Preventing and combating sexism, Recommendation CM/Rec(2019)1. https://rm.coe.int/cm-rec-2019-1-on-preventing-and-combating-sexism/168094d894

Council of Europe Gender Equality Strategy 2018-2023 https://edoc.coe.int/en/gender-equality/8111-council-of-europe-gender-equality-strategy-2018-2023.html

Gender Equality Strategy 2024-2029 https://www.coe.int/en/web/genderequality/gender-equality-strategy

European Convention on Human Rights, The Convention for the Protection of Human Rights and Fundamental Freedoms. https://www.echr.coe.int/european-convention-on-human-rights

Center for Democracy and Technology, CDT Europe Reacts to EU Directive on Gender-Based Violence (GBV), New Rules to Tackle Online GBV Create Free Expression Concerns. https://cdt.org/insights/cdt-europe-reacts-to-eu-directive-on-gender-based-violence-gbv-new-rules-to-tackle-online-gbv-create-free-expression-concerns/

Directive 2012/29/EU 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 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0029

Communication EU Strategy on victims' rights (2020-2025) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0258

Commission Staff Working Document Evaluation of 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. SWD(2022) 180 final https://commission.europa.eu/system/files/2022-06/swd_2022_179_evaluation_rep_en.pdf

Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0036

Council conclusions on combating the sexual abuse of children - Council conclusions (8 October 2019) https://data.consilium.europa.eu/doc/document/ST-12862-2019-INIT/en/pdf

Regulation (EU) 2022/2065 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A277%3ATOC&uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG

Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Amendments 1-281, Draft report Axel Voss (PE680.928v01-00) on artificial intelligence in a digital age (2020/2266(INI) https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/AIDA/AM/2022/01-13/1245944EN.pdf

Directive (EU) 2022/2381 of 23 November 2022 on improving the gender balance among directors of listed companies and related measures. https://eur-lex.europa.eu/eli/dir/2022/2381/oj

Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

European Parliament, Media Freedom Act: a new bill to protect EU journalists and press freedom. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093

Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013

Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0913

Directive 2006/54/EC on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0054

Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000L0031

Proposal for an ePrivacy Regulation https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation

European Parliament resolution of 11 March 2021 on children's rights in view of the EU Strategy on the rights of the child. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0090_EN.html

European Parliament (2021), Implementation of the Anti-Trafficking Directive https://www.europarl.europa.eu/doceo/document/TA-9-2021-0041_EN.html

European Parliament (2020), Strengthening Media Freedom: the Protection of Journalists in Europe, Hate Speech, Disinformation and the Role of Platforms https://www.europarl.europa.eu/doceo/document/TA-9-2020-0320_EN.html

European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI)) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0238

European Commission, Gender equality strategy 2020-2025 https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/gender-equality/gender-equality-strategy_en

European Commission, EU Strategy on victims' rights (2020-2025) https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/criminal-justice/protecting-victims-rights/eu-strategy-victims-rights-2020-2025_en

European Commission, EU Strategy for a more effective fight against child sexual abuse https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en

European Commission, The Cybersecurity Strategy https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Communication on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0171

European Parliament resolution of 15 June 2017 on online platforms and the digital single market https://www.europarl.europa.eu/doceo/document/TA-8-2017-0272_EN.html

2018 Code of Practice on Disinformation https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

The EU Code of conduct on countering illegal hate speech online https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0913

The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae

Rothermel, A.-K. (2023). The role of evidence-based misogyny in antifeminist online communities of the 'manosphere'. Big Data & Society, 10(1). https://doi.org/10.1177/20539517221145671

Rigsadvokatmeddelelsen 'Digitale sexkrænkelser' issued on the 1 of July 2020 is available here in Danish: https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/870f993d-5cd4-4043-9d1d-30f4200d3132?showExact=true#37bb3a605b

GREVIO Baseline Evaluation Report Portugal (2019) https://rm.coe.int/grevio-reprt-on-portugal/168091f16f

Mary Anne Franks & Ari Ezra Waldman (2019), Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions, 78 Md. L. Rev. 892, 893

Report on extending the list of EU crimes to hate speech and hate crime (2023) https://www.europarl.europa.eu/doceo/document/A-9-2023-0377_EN.html

Jamie Achtmeyer (2022), Pickup Artistry: an Exploration of Hypersexuality and Toxic Masculinity https://qc-writers.com/2022/05/08/1849/

Annex II
List of consulted stakeholders

Interview with **Eleonora Esposito**, Case Handler Officer in the Digital Services Unit of DG CONNECT, carried out on 16.02.2024.

Interview with **Sara De Vido**, Associate Professor at Ca' Foscari University of Venice, carried out on 12.02.2024.

Interview with **Silvia Semenzin**, Post-doctoral researcher in Digital Sociology at the University of Computer Science of Madrid and human rights activist, carried out on 23.02.2024.

Interview with **Pille Psopp-Pagan**, Member of GREVIO, carried out on 15.02.2024.

Interview with **Maria João Faustino**, Post-Doctoral Researcher at the Center for Social Studies of the University of Coimbra, carried out on 18.03.2024.

ENDNOTES

[1] United States, Committee On Oversight and Accountability, Cybersecurity, Information Technology, and Government Innovation Subcommittee (2024), Hearing on Addressing Real Harm Done by Deepfakes. https://oversight.house.gov/hearing/addressing-real-harm-done-by-deepfakes/

[2] MA. Chen, Three Threats Posed by Deepfakes That Technology Won't Solve (2019), MIT Technology Review. https://www.technologyreview.com/2019/10/02/75400/deepfake-technology-detection-disinformation-harassment-revenge-porn-law/; See also M. A. Franks, Hearing on Addressing Real Harm Done by Deepfakes' (2024) U.S. Congress https://www.congress.gov/118/meeting/house/116953/documents/HHRG-118-GO12-20240312-SD008.pdf

[3] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[4] Ibid.

[5] EU Directive 2024/1385 on combating violence against women and domestic violence. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401385

[6] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[7] United Nations, Sustainable Development Goals, The Sustainable Development Agenda. https://www.un.org/sustainabledevelopment/development-agenda/

[8] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[9] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[10] UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[11] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and

Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[12] European Women's Lobby (EWL) (2017), #HerNetHerRights, Mapping the state of online violence against women and girls in Europe. https://www.womenlobby.org/Read-and-share-HerNetHerRights-Resource-Pack-Report

[13] European Parliament Research Service (EPRS) (2021), Combating Gender based Violence: Cyber Violence. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621

[14] Ibid.

[15] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[16] UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[17] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[18] GREVIO (2021), General Recommendation No 1 on the digital dimension of violence against women, Council of Europe, Strasbourg. https://rm.coe.int/%20grevio-rec-no-on-digital-violence-against-women/1680a49147

[19] Pew Research Center (2021), The state of online harassment. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

[20] Almenar, R. (2021), Cyberviolence against women and girls: gender-based violence in the digital age and future challenges as a consequence of Covid-19, Trento Student Law Review Association, Vol. 3, No 1, Trento, Italy, pp. 167–230. https://teseo.unitn.it/tslr/article/view/757

[21] Ibid.

[22] World Wide Web Foundation (2021), Online Gender-Based Violence and Abuse: Consultation Briefing. https://uploads-ssl.webflow.com/61557f76c8a63ae527a819e6/615585a9bbfeb8836d512947_OGBV_ConsultationBriefing.pdf

[23] European Commission (2020), Advisory Committee on Equal Opportunities for Women and Men , Opinion on combatting online violence against women, Brussels. https://commission.europa.eu/system/files/2024-01/Opinion%20violence%20adopted.pdf

[24] Professor Liz Kelly was the first to establish the concept of a 'continuum of violence' in her book 'Surviving Sexual Violence'(1st ed.)(1988). Polity.

[25] European Parliament Research Service (EPRS) (2021), Combating Gender based Violence: Cyber Violence. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621

[26] GREVIO (2021), General Recommendation No 1 on the digital dimension of violence against women, Council of Europe, Strasbourg. https://rm.coe.int/%20grevio-rec-no-on-digital-violence-against-women/1680a49147

[27] United Nations (2022), Report of Secretary General, Intensification of efforts to eliminate all forms of violence against women and girls. A/77/302.

[28] Rigotti, C. and Al. (2023), Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. Published in: New Journal of European Criminal Law. https://cris.vub.be/ws/portalfiles/portal/92354738/20322844221140713.pdf

[29] GREVIO (2021), General Recommendation No 1 on the digital dimension of violence against women, Council of Europe, Strasbourg. https://rm.coe.int/%20grevio-rec-no-on-digital-violence-against-women/1680a49147

[30] This definition comprises 'all acts of gender-based violence against women that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life'.
Council of Europe (2014), Convention on preventing and combating violence against women and domestic violence (Instanbul Convention). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210

[31] UN Human Rights Council (18 June 2018), 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, A/HRC/38/47. https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and

[32] UN Women (2023), Technology-Facilitated Violence Against Women: Taking Stock Of Evidence And Data Collection. https://www.unwomen.org/en/digital-library/publications/2023/04/technology-facilitated-violence-against-women-taking-stock-of-evidence-and-data-collection

[33] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[34] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[35] UN Women (2023), Technology-Facilitated Violence Against Women: Taking Stock Of Evidence And Data Collection. https://www.unwomen.org/en/digital-li-

brary/publications/2023/04/technology-facilitated-violence-against-women-taking-stock-of-evidence-and-data-collection

[36] GREVIO (2021), General Recommendation No 1 on the digital dimension of violence against women, Council of Europe, Strasbourg. https://rm.coe.int/%20grevio-rec-no-on-digital-violence-against-women/1680a49147

[37] UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls.https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[38] Ibid.

[39] The Economist Intelligence Unit (2021), Measuring the Prevalence of Online Violence against Women. https://onlineviolencewomen.eiu.com/ A survey was conducted across 45 countries (a sample of 100 replies for each country).

[40] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[41] United Nations Population Fund (UNFPA), (2021), Making all spaces safe. New York. https://www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe

[42] Smith, G., & Rustagi, I. (2021). When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity. Stanford Social Innovation Review. https://doi.org/10.48558/A179-B138

[43] United Nations (2023), How Technology-Facilitated Gender-Based Violence Impacts Women and Girls. https://unric.org/en/how-technology-facilitated-gender-based-violence-impacts-women-and-girls/

[44] European Parliament Research Service (EPRS) (2021), Combating Gender based Violence: Cyber Violence. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621
The EPRS's study refers to deepfakes, whereas the EWL refers to sexual digital forgeries and digital forgeries, see Note on terminology of this report at the beginning of the report.

[45] World Economic Forum (2024), The Global Risk Report 2024.
https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

[46] The Conversation, Deepfakes: How to empower youth to fight the threat of misinformation and disinformation
https://theconversation.com/deepfakes-how-to-empower-youth-to-fight-the-threat-of-misinformation-and-disinformation-22117

[47] EPRS, (2021), Combating Gender based Violence: Cyber Violence. https://www.europarl.europa.eu/thinktank/en/document/EPRS_

STU(2021)662621. The EPRS's study refers to deepfakes, whereas the EWL refers to sexual digital forgeries and digital forgeries, see Note on terminology of this report at the beginning of the report.

[48] Ibid.

[49] Ibid.

[50] Ibid. The EPRS (2021) study refers to 'pornographic videos'; however, the EWL prefers to use the term sexual abuse.

[51] Ibid. The EPRS (2021) study refers to 'Non-consensual pornographic deepfakes', however, the EWL prefers to use the term sexual digital forgeries.

[52] Patrini, Georgio (2019), Mapping the Deepfake Landscape. Sensity. The source refers to 'material depicting pornography', however the EWL prefers to refer to 'material depicting nudity or sexually explicit activities'. See Notes on terminology of this report at the beginning of the report. https://giorgiop.github.io/posts/2018/03/17/mapping-the-deepfake-landscape/

[53] Patrini, Giorgio (2020). Automating Image Abuse: Deepfake Bots on Telegram. Sensity (blog), 2020. https://sensity.ai/automating-image-abuse-deepfake-bots-on-telegram/. The source refers to deepfakes, whereas the EWL refers to sexual digital forgeries and digital forgeries, see Notes on terminology of this report at the beginning of the report.

[54] Ibid. The EPRS (2021) study refers to 'Non-consensual pornographic deepfakes', however, the EWL prefers to use the term sexual digital forgeries. See Notes on terminology of this report at the beginning of the report.

[55] EPRS, (2021), Combating Gender based Violence: Cyber Violence. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621. The study refers to deepfake pornography, whereas the EWL refers to sexual digital forgeries and digital forgeries, see Notes on terminology of this report at the beginning of the report.

[56] John Villasenor, Artificial intelligence, deepfakes, and the uncertain future of truth. https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/ The source refers to deepfakes, whereas the EWL refers to sexual digital forgeries and digital forgeries, see Notes on terminology of this report at the beginning of the report.

[57] Equality Now (2023), Briefing Paper: Deepfake Image-Based Sexual Abuse, Tech-Facilitated Sexual Exploitation And The Law. The source refers to deepfakes, whereas the EWL refers to sexual digital forgeries and digital forgeries, see Notes on terminology of this report at the beginning of the report.

[58] Cyber Rights organisation, NCII: 90% of victims of the distribution of non-consensual intimate imagery are women. https://cyberights.org/ncii-90-of-victims-of-the-distribution-of-non-consensual-intimate-imagery-are-women/

[59] Van de Heyning C. et al. (2023), Les Deepnudes Parmi Les Jeunes Belges. Bruxelles.

https://igvm-iefh.belgium.be/sites/default/files/les_deepnudes_parmi_les_jeunes_belges.pdf

[60] European Institute for Gender Equality (EIGE) (2021), Artificial intelligence, platform work and gender equality. https://eige.europa.eu/publications-resources/publications/artificial-intelligence-platform-work-and-gender-equality?language_content_entity=en#:~:text=The%20growth%20of%20artificial%20intelligence,discrimination%20in%20the%20labour%20market.

[61] EPRS, (2021), Combating Gender based Violence: Cyber Violence. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621

[62] Technology that collects, analyses and applies data, and uses this to place digital layers over the physical reality in order to create 'hybrid' worlds. These are simultaneously physical and virtual. The technology is used for popular apps such as Snapchat and Pokémon Go.

[63] Monash University, Sexual assault in the metaverse is part of a bigger problem that technology alone won't solve. https://lens.monash.edu/@politics-society/2022/07/22/1384871/sexual-assault-in-the-metaverse-theres-nothing-virtual-about-it

[64] Leonard D. J. (2019). Virtual anti-racism: Pleasure, catharsis, and hope in Mafia III and Watch Dogs 2. Humanity and Society, 44(1), 111–130. https://doi.org/10.1177/0160597619835863

[65] Wiederhold B.K., (2022). Sexual Harassment in the Metaverse. https://www.liebertpub.com/doi/full/10.1089/cyber.2022.29253.editorial

[66] Singh K. (2022). In the metaverse, sexual assault is very real. So what can we do legally? https://www.refinery29.com

[67] Jenson J., De Castell S. (2021). Patriarchy in play: Video games as gendered media ecologies. Explorations in Media Ecology, 20(2), 195–212. https://doi.org/10.1386/eme_00084_1

[68] Macêdo Callou, R.C. et al. (2021), Cyberbullying and gender violence in online games. https://www.researchgate.net/publication/352330454_Cyberbullying_and_gender_violence_in_online_games

[69] Supplemental Digital Content 2, Summary of research Studies addressing VR/Gaming and Sexual Violence related. https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fcdn-links.lww.com%2Fpermalink%2Fjfn%2Fa%2Fj-fn_00_00_2023_10_23_porta_jfn-23-061_sdc2.docx&wdOrigin=BROWSELINK

[70] Information confirmed by a representative of DG Connect (interview carried out on 16.02.2024).

[71] Jagavat. A. et al. (2021) Cyber-aggression towards women: Measurement and psychological predictors in gaming communities. Department of Psychology, Toronto.

[72] Porta, C. et al. (2024), Sexual Violence in Virtual Reality, A Scoping Review. Journal of Forensic Nursing 20(1):p 66-77, 1/3 2024. https://journals.lww.com/forensicnursing/fu-

lltext/2024/03000/sexual_violence_in_virtual_reality__a_scoping.8.aspx

[73] Jagavat. A. et al. (2021) Cyber-aggression towards women: Measurement and psychological predictors in gaming communities. Department of Psychology, Toronto.

[74] Gray, K.L. et al. (2017), Blurring the boundaries: Using Gamergate to examine 'real' and symbolic violence against women in contemporary gaming culture. Sociology Compass.

[75] Tang, W. Y., Reer, F., & Quandt, T. (2020). The interplay of gaming disorder, gaming motivations, and the dark triad. Journal of Behavioral Addictions, 9(2), 491–496. https://akjournals.com/view/journals/2006/9/2/article-p491.xml

[76] Ibid.

[77] UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[78] Europol (2020), Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. https://www.europol.europa.eu/publications-events/publications/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic

[79] Council of Europe (2014), Convention on preventing and combating violence against women and domestic violence (Istanbul Convention). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210

[80] Council of Europe (2014), Convention on preventing and combating violence against women and domestic violence (Istanbul Convention). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210

[81] FRA (European Union Agency for Fundamental Rights) (2014), Violence against Women: An EU-wide survey – Main results report, Publications Office of the European Union, Luxembourg. https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

[82] The Economist Intelligence Unit (2021), Measuring the Prevalence of Online Violence against Women. https://onlineviolencewomen.eiu.com/ A survey was conducted across 45 countries (a sample of 100 replies for each country).

[83] Council of Europe, Cybercrime, Council of Europe Cybercrime Convention Committee, 2018.

[84] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[85] FRA (European Union Agency for Fundamental Rights) (2014), Violence against Women: An EU-wide survey – Main results report, Publications Office of the European Union, Luxembourg. https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

[86] FRA (2021), Crime Safety and victims rights. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-crime-safety-victims-rights_en.pdf

[87] EIGE (W2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[88] For example, according to McGlynn, C. et al, image-based sexual abuse refers to the taking or sharing of nude or sexual photographs or videos of another person without their consent. It includes a diversity of behaviours beyond that of 'revenge porn', such as the secret trading of nude or sexual images online; 'upskirting', 'downblousing' and other 'creepshots'; blackmail or 'sextortion' scams; the use of artificial intelligence to construct 'deepfake pornographic videos; threats to distribute photographs and videos without consent; and the taking or sharing of sexual assault imagery. (Henry et al., Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery (n 13) 11.)

[89] McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. Oxford Journal of Legal Studies, 37(3), 534-561.

[90] Expert Opinion by Professor Clare McGlynn, Durham Law School, Durham University, UK and Professor Lorna Woods, School of Law, University of Essex, UK (2022), Image-Based Sexual Abuse, Pornography Platforms and the Digital Services Act. https://hateaid.org/wp-content/uploads/2022/04/ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf

[91] Quoted in EIGE (European Institute for Gender Equality) (2022), Combating cyber violence against women and girls, Vilnius.

[92] Ruvalcaba, Y., & Eaton, A. A. (2019), Non consensual pornography among U.S. adults: A sexual scripts framework on victimization, perpetration, and health correlates for women and men. Psychology of Violence. https://doi.org/10.1037/vio0000233

[93] ECtHR (2023), Factsheet – Hate speech, available at https://www.echr.coe.int/documents/d/echr/FS_Hate_speech_ENG

[94] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[95] Rothermel, A.-K. (2023). The role of evidence-based misogyny in antifeminist online communities of the 'manosphere'. Big Data & Society, 10(1). https://doi.org/10.1177/20539517221145671

[96] Jamie Achtmeyer, Pickup Artistry: an Exploration of Hypersexuality and Toxic Masculinity. https://qc-writers.com/2022/05/08/1849/

[97] European Commission (2021), Incels: A First Scan of the Phenomenon (in the EU) and its Relevance and Challenges for P/CVE. https://home-affairs.ec.europa.eu/system/files/2021-10/ran_incels_first_scan_of_phe-

nomen_and_relevance_challenges_for_p-cve_202110_en.pdf

[98] Inés Abalo Rodríguez y Mónica Alario Gavilán (2024), Impact of male pornography Consumption on the Perpetration of sexual violence. https://lobbyeuropeoespana.com/wp-content/uploads/2024/04/11-abril-version-ingles-digital-interactiva-impacto-del-consumo-masculino-de-pornografia.pdf

[99] Baron & Straus (1984), in Mary Anne Layden, Pornography and Violence: a new look at research (2009). https://www.socialcostsofpornography.com/Layden_Pornography_and_Violence.pdf

[100] Utah Domestic Violence Coalition, 2009, available at: https://udvc.org/. Silbert & Pines, 1984: In her research with 200 women in prostitution, Mimi Silbert recognised the role played by pornography in legitimising victimisation; in the account of rape, almost a quarter of these women made reference to pornography used by the rapist.

[101] Inés Abalo Rodríguez y Mónica Alario Gavilán (2024), Impact of male pornography Consumption on the Perpetration of sexual violence. https://lobbyeuropeoespana.com/wp-content/uploads/2024/04/11-abril-version-ingles-digital-interactiva-impacto-del-consumo-masculino-de-pornografia.pdf

[102] French Senate Delegation of women's rights and equal opportunities between men and women (2022), Focus on Porn: hell behind the scenes. https://www.senat.fr/fileadmin/Fichiers/Images/delegation/femmes/L_Essentiel_Porno_ENGLISH.pdf

[103] UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls.https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[104] The Economist Intelligence Unit (2021), Measuring the Prevalence of Online Violence against Women. https://onlineviolencewomen.eiu.com/ A survey was conducted across 45 countries (a sample of 100 replies for each country).

[105] Hicks, J. (2021), Global evidence on the prevalence and impact of online gender-based violence (OGBV).

[106] The Economist Intelligence Unit (2021), Measuring the Prevalence of Online Violence against Women. https://onlineviolencewomen.eiu.com/ A survey was conducted across 45 countries (a sample of 100 replies for each country).

[107] Ibid.

[108] The Economist Intelligence Unit (2021), Measuring the Prevalence of Online Violence against Women. https://onlineviolencewomen.eiu.com/ A survey was conducted across 45 countries (a sample of 100 replies for each country).

[109] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-di-

gitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[110] Forms of TF VAW in the survey included receiving inappropriate sexual advances or sexual content on social networking websites, pressure to share sexually suggestive or explicit images or messages, sharing or threatening to share personal or intimate content without their consent, monitoring their digital communication or location, and other acts.

[111] UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[112] World Wide Web Foundation (2020), There's a pandemic of online violence against women and girls. https://webfoundation.org/2020/07/theres-a-pandemic-of-online-violence-against-women-and-girls/

[113] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[114] FRA (European Union Agency for Fundamental Rights) (2014), Violence against Women: An EU-wide survey – Main results report, Publications Office of the European Union, Luxembourg.

[115] FRA (2021), Crime Safety and victims rights. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-crime-safety-victims-rights_en.pdf

[116] HateAid (2021), Boundless hate on the internet – Dramatic situation across Europe. https://hateaid.org/wp-content/uploads/2022/04/HateAid-Report-2021_EN.pdf

[117] Ibid.

[118] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[119] Bumble (2023), Bumble Backs Law to Ban Cyberflashing in 27 Countries https://bumble.com/en/the-buzz/bumble-backs-law-to-ban-cyberflashing-27-countries-eu-europe

[120] Ipsos (2021), Les Français et le cyberharcèlement Ampleur du phénomène, conséquences, préoccupations et idées reçues. https://www.ipsos.com/sites/default/files/ct/news/documents/2021-12/Enquete%20Ipsos-Meetic.pdf

[121] UN Women (2023), The State of Evidence and Data Collection on Technology-facilitated Violence against Women. https://www.unwomen.org/sites/default/files/2023-04/Brief-The-state-of-evidence-and-data-collection-on-technology-facilitated-violence-against-women-en.pdf

[122] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-di-

gitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[123] Security (2024), Cyberbullying: Twenty Crucial Statistics for 2024 https://www.security.org/resources/cyberbullying-facts-statistics/

[124] Ipsos (2022), Etude sur les cyberviolences et le cyberharcelement volet victimes, https://drive.google.com/file/d/1uaWxIgLY7p2tc7Rv6DnkCMfOKEDgwxK6/view

[125] Amnesty International (2018), Toxic Twitter - A Toxic Place for Women. https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1-1/

[126] UN Women (2023), The State of Evidence and Data Collection on Technology-facilitated Violence against Women. https://www.unwomen.org/sites/default/files/2023-04/Brief-The-state-of-evidence-and-data-collection-on-technology-facilitated-violence-against-women-en.pdf

[127] Ibid.

[128] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[129] Gurumurthy, A., Vasudevan, A. & Chami, N. (2019), Born digital, born free? A socio-legal study on young women's experiences of online violence in South India. IT for Change. https://itforchange.net/sites/default/files/1662/Born-Digital_Born-Free_SynthesisReport.pdf

[130] European Women's Lobby (2023), Feminist Sexuality Education. https://www.womenlobby.org/IMG/pdf/lef_sexeduc_web.pdf

[131] Expert Opinion by Professor Clare McGlynn, Durham Law School, Durham University, UK and Professor Lorna Woods, School of Law, University of Essex (UK) (2022). Image-Based Sexual Abuse, Pornography Platforms and the Digital Services Act. https://hateaid.org/wp-content/uploads/2022/04/ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf

[132] Vera-Gray, F., McGlynn, C., Kureshi, I., & Butterby, K. (2021). Sexual violence as a sexual script in mainstream online pornography. The British Journal of Criminology, 61(5), 1243-1260.

[133] Expert Opinion by Professor Clare McGlynn, Durham Law School, Durham University, UK and Professor Lorna Woods, School of Law, University of Essex (UK) (2022). Image-Based Sexual Abuse, Pornography Platforms and the Digital Services Act. https://hateaid.org/wp-content/uploads/2022/04/ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf

[134] Vera-Gray, F. McGlynn, C. et al. (2021), Sexual violence as a sexual script in mainstream online pornography. The British Journal of Criminology, Volume 61, Issue 5, September 2021,

Pages 1243–1260.
https://doi.org/10.1093/bjc/azab035

[135] UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls.https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[136] FRA (2023), Online Content Moderation – Current challenges in detecting hate speech. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-online-content-moderation_en.pdf

[137] Pew Research Centre, (2021), The state of online harassment. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

[138] Ibid.

[139] United Nations, Digital Library, (2018) 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. https://digitallibrary.un.org/record/1641160?ln=en&v=pdf

[140] The global partnership, (2023), Technology-Facilitated Gender-Based Violence: Preliminary Landscape Analysis. https://www.gov.uk/government/publications/technology-facilitated-gender-based-violence-preliminary-landscape-analysis

[141] eSafety Commissioner Australia (2021), 'For My Safety': Experiences of Technology-Facilitated Abuse among Women with Intellectual Disability or Cognitive Disability. https://www.esafety.gov.au/sites/default/files/2021-09/TFA%20WWICD_accessible.pdf

[142] Vox, Osservatorio Italiano sui Diritti, La nuova Mappa dell'Intolleranza 7. http://www.voxdiritti.it/la-nuova-mappa-dellintolleranza-7/

[143] Amnesty Interternational (2018), Toxic Twitter - Triggers of Violence and Abuse Against Women on Twitter. https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2-3/

[144] European Disability Forum (EDF) (2023), The digital dimension of gender-based violence. https://www.edf-feph.org/blog/the-digital-dimension-of-gender-based-violence/

[145] EPRS (2021), Combating Gender-based Violence: Cyber violence – European added value assessment. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf

[146] Council of Europe, Commissioner for Human Rights (2022), No space for violence against women and girls in the digital world. https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

[147] FRA (2017), Challenges to Women's Human Rights in the EU – Gender discrimination, sexist hate speech and gender-based violence against women and girls, Publications Office of the European Union, Luxembourg. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-cha-

llenges-to-women-human-rights_en.pdf

[148] UNESCO (2020), Online violence against women journalists: a global snapshot of incidence and impacts. https://unesdoc.unesco.org/ark:/48223/pf0000375136

[149] National Democratic Institute (2019), Tweets That Chill: Analyzing Online Violence Against Women in Politics. https://www.ndi.org/sites/default/files/NDI%20Tweets%20That%20Chill%20Report.pdf

[150] European Parliament, Violence against women active in politics in the EU. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/759600/EPRS_BRI(2024)759600_EN.pdf

[151] National Democratic Institute (2019), Tweets That Chill: Analyzing Online Violence Against Women in Politics. https://www.ndi.org/sites/default/files/NDI%20Tweets%20That%20Chill%20Report.pdf

[152] World Wide Web Foundation (2021), Online Gender-Based Violence and Abuse: Consultation Briefing. https://webfoundation.org/our-work/projects/tackling-online-gender-based-violence-and-abuse-against-women/

[153] Plan International (2020), Free to Be Online? https://plan-international.org/publications/free-to-be-online/

[154] World Wide Web Foundation and World Association of Girl Guides and Girl Scouts (2020), Survey Young People's Experience of Online Harassment. https://webfoundation.org/docs/2020/03/WF_WAGGGS-Survey-1-pager-1.pdf

[155] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en.

[156] Ibid.

[157] Henry, N., McGlynn, C. et. Al (2020), Image-based Sexual Abuse, A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery.

[158] On the trading of nude images of women without their knowledge, see: 'Inside the Secret World of Trading Nudes' BBC News (London, 22 August 2022).

[159] Plan International (2020), Free to Be Online? https://plan-international.org/publications/free-to-be-online/

[160] Amnesty Interternational (2018), Toxic Twitter - Triggers of Violence and Abuse Against Women on Twitter. https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2-3/

[161] Bailey L. et Al (2023), The Networking of Abuse: Intimate Partner Violence and the Use of Social Technologies, Volume 51, Issue 2. https://orcid.org/0000-0002-1498-2485
Fraser, C., et al. (2010), The New Age of Stalking: Technological Implications for Stalking, Juvenile and Family Court Journal. https://www.researchgate.net/publication/229636491_The_New_Age_of_Stalking_Technological_Implications_for_Stalking

[162] Flynn A. et al. (2021), Technology-facilitated

abuse. Technology-facilitated abuse: A survey of support services stakeholders. https://www.anrows.org.au/publication/technology-facilitated-abuse-a-survey-of-support-services-stakeholders/

[163] Ibid.

[164] Parsons et Al. (2019), The Predator in Your Pocket. A Multidisciplinary Assessment of the Stalkerware Application Industry, University of Toronto, https://tspace.library.utoronto.ca/bitstream/1807/96320/1/stalkerware-holistic.pdf

[165] UNFPA (2021), Technology-facilitated Gender-based Violence: Making All Spaces Safe. https://www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe

[166] Iyer, N. et Al. (2020), Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet. APC and IDRC.

[167] UN Expert Group (2023), Technology-facilitated Violence against Women: Towards a common definition Report of the meeting of the Expert Group 15-16 November 2022, New York, USA. https://www.unwomen.org/en/digital-library/publications/2023/03/expert-group-meeting-report-technology-facilitated-violence-against-women

[168] UNFPA (2021), Technology-facilitated Gender-based Violence: Making All Spaces Safe. https://www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe

[169] EPRS (2021), Combating Gender-based Violence: Cyber violence – European added value assessment. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf

[170] Ibid.

[171] GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence. Learning Brief 1: Understanding technology-facilitated GBV. Several cases of suicide are documented, see for example https://www.bbc.com/news/world-europe-37380704

[172] Several cases of suicide among victims of CVAW are documented, see for example: https://www.bbc.com/news/world-europe-37380704; https://www.elindependiente.com/sociedad/2020/05/25/archivan-el-caso-del-suicidio-de-la-empleada-de-iveco-al-no-descubrirse-quien-difundio-su-video-sexual/

[173] Amnesty Interternational (2018), Toxic Twitter - Triggers of Violence and Abuse Against Women on Twitter. https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2-3/

[174] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[175] McGlynn, C. et Al., 'It's torture for the soul': the harms of image-based sexual abuse', So-

cial and Legal Studies, vol. 30, No. 4, (2021), pp. 541–562.

[176] Plan International (2020), Free to Be Online? https://plan-international.org/publications/free-to-be-online/

[177] UNFPA (2021), Technology-facilitated Gender-based Violence: Making All Spaces Safe. https://www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe

[178] Amnesty International (2017), Amnesty reveals alarming impact of online abuse against women. https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women-2/

[179] The European Liberal Forum (2021), Violence Against Women In European Politics. https://liberalforum.eu/wp-content/uploads/2022/01/violence-against-women-in-european-politics_final.pdf

[180] Hicks, J. (2021), Global evidence on the prevalence and impact of online gender-based violence (OGBV). https://www.ids.ac.uk/publications/global-evidence-on-the-prevalence-and-impact-of-online-gender-based-violence-ogbv/

[181] Posetti, J., et AL. (2021), The chilling: Global trends in online violence against women journalists. UNESCO Research Discussion Paper. https://unesdoc.unesco.org/ark:/48223/pf0000377223/PDF/377223eng.pdf.multi

[182] World Wide Web Foundation, (2021). Tech Policy Design Lab: Online Gender-Based Violence and Abuse: Outcomes and Recommendations. https://techlab.webfoundation.org/ogbv/overview

[183] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia.UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[184] Council of Europe (2014), Convention on preventing and combating violence against women and domestic violence (Istanbul Convention). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210

[185] European Parliament, EU accession to the Istanbul Convention. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739323/EPRS_ATA(2023)739323_EN.pdf

[186] Council of Europe (2011), Explanatory report to the Council of Europe Convention on preventing and combating violence against women and domestic violence, Council of Europe Treaty Series, No 210 https://rm.coe.int/%20ic-and-explanatory-report/16808d24c6

[187] GREVIO (2021), General Recommendation No 1 on the digital dimension of violence against women, Council of Europe, Strasbourg. https://rm.coe.int/%20grevio-rec-no-on-digital-violence-against-women/1680a49147

[188] EJIL:Talk! (2022), The Istanbul Convention: A Missed Opportunity in Mainstreaming Cyber-violence against Women in Human Rights Law? https://www.ejiltalk.org/the-istanbul-convention-a-missed-opportunity-in-mainstreaming-cyberviolence-against-women-in-human-rights-law/

[189] Directive 2024/1385 on combating violence against women and domestic violence. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401385

[190] EWL, European Women's Lobby work on the EU Directive on violence against women, https://womenlobby.org/EU-Directive-on-violence-against-women?lang=en

[191] A list of the consulted stakeholders is provided in Annex II.

[192] Rigotti, C. and Al. (2023), Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. Published in: New Journal of European Criminal Law. https://cris.vub.be/ws/portalfiles/portal/92354738/20322844221140713.pdf

[193] Art. 11 refers to offences from Art. 6 till 9b.

[194] EWL (2024), European Women's Lobby work on the EU Directive on violence against women, https://womenlobby.org/EU-Directive-on-violence-against-women?lang=en

[195] FRA (European Union Agency for Fundamental Rights) (2014), Violence against Women: An EU-wide survey – Main results report, Publications Office of the European Union, Luxembourg. https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

[196] EWL (2023), EWL Observatory Analysis of definitions of rape in the EU- The added value the EU Directive on VAW. https://womenlobby.org/EWL-Observatory-Analysis-of-definitions-of-rape-in-the-EU-The-added-value-of?lang=en

[197] See for example, GenderIT, Navigating Policy Designs: A Case for Specific and Broad Policies to Counter New Forms of Technology-Facilitated Violence. https://genderit.org/articles/navigating-policy-designs-case-specific-and-broad-policies-counter-new-forms-technology

[198] EWL (2023), EWL Priorities for the Trilogues: Rape must be made an offence under the Directive on violence against women. https://www.womenlobby.org/EWL-Priorities-for-the-interinstitutional-negotiations?lang=en

[199] Ibid.

[200] Rigotti, C. and Al. (2023), Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. Published in: New Journal of European Criminal Law. https://cris.vub.be/ws/portalfiles/portal/92354738/20322844221140713.pdf

[201] Ibid.

[202] Ibid.

[203] Ibid.

[204] Center for Democracy and Technology (CDT), Europe Reacts to EU Directive on Gender-Based Violence (GBV), New Rules to Tackle Online GBV Create Free Expression Concerns. https://cdt.org/insights/cdt-europe-reacts-to-eu-directive-on-gender-based-violence-gbv-new-rules-to-tackle-online-gbv-create-free-expression-concerns/

[205] Directive 2012/29 establishing minimum standards on the rights, support and protection of victims of crime. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0029

[206] European Commission, Commission proposes to strengthen the rights of victims of crime. https://ec.europa.eu/commission/presscorner/api/files/document/print/%20nl/ip_23_3724/IP_23_3724_EN.pdf

[207] Communication on the EU Strategy on victims' rights (2020-2025) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0258

[208] Commission Staff Working Document Evaluation of Directive 2012/29/EU stablishing minimum standards on the rights, support and protection of victims of crime. https://commission.europa.eu/system/files/2022-06/swd_2022_179_evaluation_rep_en.pdf

[209] Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0036

[210] Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0036

[211] Council of the EU (2019), Council conclusions on combating the sexual abuse of children; https://data.consilium.europa.eu/doc/document/ST-12862-2019-INIT/en/pdf

[212] Europol (2020), The challenges of countering human trafficking in the digital era. https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf

[213] Regulation (EU) 2022/2065 on a Single Market For Digital Services (Digital Services Act). https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[214] European Parliament Research Service (EPRS) (2021), Tackling deepfakes in European policy. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

[215] FRA (2023), Online Content Moderation – Current challenges in detecting hate speech. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-online-content-moderation_en.pdf

[216] Interview with Eleonora Esposito from DG Connect, carried out on 17.02.2024.

[217] Expert Opinion by Professor Clare McGlynn, Durham Law School, Durham University, UK and Professor Lorna Woods, School of Law, University of Essex, UK (2022), Image-Based Sexual Abuse, Pornography Platforms and the Digital Services Act. https://hateaid.org/wp-content/uploads/2022/04/ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf

[218] In December 2023, the European Commission launched a public consultation to gather feedback on the Implementing Regulation on the templates that intermediary services and online platforms will have to use for their future transparency reports under the Digital Services Act (DSA). Based on this feedback, the commission is analysing and developing specific categories of risks.

[219] Shaping Europe's digital future, Commission designates second set of Very Large Online Platforms under the Digital Services Act. https://digital-strategy.ec.europa.eu/en/news/commission-designates-second-set-very-large-online-platforms-under-digital-services-act

[220] While criticism has been expressed towards the text of the DSA as proposed by the Commission, it still applies with regard to the final version of the DSA.

[221] Expert Opinion by Professor Clare McGlynn, Durham Law School, Durham University, UK and Professor Lorna Woods, School of Law, University of Essex, UK (2022), Image-Based Sexual Abuse, Pornography Platforms and the Digital Services Act. https://hateaid.org/wp-content/uploads/2022/04/ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf

[222] Ibid.

[223] Turillazzi, A. et Al. (2023) The digital services act: an analysis of its ethical, legal, and social implications, Law, Innovation and Technology, 15:1, 83-106. https://www.tandfonline.com/doi/full/10.1080/17579961.2023.2184136

[224] Barker K. & Jurasz, O. (2024), Digital and online violence: international perspectives, International Review of Law, Computers & Technology. https://www.tandfonline.com/doi/full/10.1080/13600869.2023.2295088

[225] Center for Democracy and Technology (CDT) (2023), EU Tech Policy Brief. https://cdt.org/insights/eu-tech-policy-brief-july-2023/

[226] Interview with Maria João Faustino, Post-Doctoral Researcher at the Center for Social Studies of the University of Coimbra.

[227] Regulation (EU) 2024/1689 Artificial Intelligence Act. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[228] European Parliament Research Service (EPRS) (2021), Tackling deepfakes in European policy. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

[229] The EPRS Study refers to 'deepafakes'. However, the EWL prefers to use the term 'sexual digital forgeries'.

[230] Interview with a representative of DG Connect carried out on 16.02.2024.

[231] FemAI, A feminist vision for the EU AI Act. https://www.fem-ai-center-for-feminist-artificial-intelligence.com/_files/ugd/f05f97_0c369b5785d944fea2989190137835a1.pdf

[232] Draft report Axel Voss (PE680.928v01-00) on artificial intelligence in a digital age (2020/2266(INI), AMENDMENTS 1 – 281. https://www.europarl.europa.eu/meet-

docs/2014_2019/plmrep/COMMITTEES/AIDA/AM/2022/01-13/1245944EN.pdf

[233] Regulation 2016/679 General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[234] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[235] European Parliament Research Service (EPRS) (2021), Tackling deepfakes in European policy. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf The source refers to deepfakes whereas EWL prefers to use the term sexual digital forgeries and digital forgeries, see Notes on terminology at the beginning of this report.

[236] For a more detailed analysis, see EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[237] Combating gender-based violence: cyber violence - Legislative Train Schedule. https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-combating-gender-based-cyber-violence

[238] European Parliament resolution of 11 March 2021 on children's rights in view of the EU Strategy on the rights of the child. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0090_EN.html

[239] Implementation of the Anti-Trafficking Directive, 10 February 2021. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0041_EN.html

[240] Strengthening Media Freedom: the Protection of Journalists in Europe, Hate Speech, Disinformation and the Role of Platforms (2020) https://www.europarl.europa.eu/doceo/document/TA-9-2020-0320_EN.html

[241] European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI)) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0238

[242] European Parliament, Resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector'. P9_TA(2021)0238 May 19th 2021.

[243] European Parliament, Report on intellectual property rights for the development of artificial intelligence technologies.' P9_TA (2020)0277 October 20th 2020.

[244] European Commission, Gender equality strategy. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/gender-equality/gender-equality-strategy_en

[245] European Commission, EU Strategy on victims' rights (2020-2025). https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/criminal-justice/protecting-victims-rights/eu-strategy-victims-rights-2020-2025_en

[246] European Commission, EU Strategy for a

more effective fight against child sexual abuse. https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en

[247] European Commission, The Cybersecurity Strategy. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[248] Commnication on the EU Strategy on Combatting Trafficking in Human Beings 2021- 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0171

[249] Tech Accord to Combat Deceptive Use of AI in 2024 Elections

[250] Code of Conduct for the 2024 European Parliament Elections

[251] European Parliament resolution of 15 June 2017 on online platforms and the digital single market https://www.europarl.europa.eu/doceo/document/TA-8-2017-0272_EN.html

[252] Summary report of the public consultation on fake news and online disinformation https://digital-strategy.ec.europa.eu/en/library/summary-report-public-consultation-fake-news-and-online-disinformation#:~:text=The%20public%20consultation%20took%20place%20between%2013%20November,actions%20to%20address%20different%20types%20of%20fake%20news.

[253] Final report of the High Level Expert Group on Fake News and Online Disinformation https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation

[254] European Commission, 2018 Code of Practice on Disinformation. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

[255] European Parliament Research Service (EPRS) (2021), Tackling deepfakes in European policy. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

[256] European Commission, The EU Code of conduct on countering illegal hate speech online. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[257] Ibid.

[258] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0913

[259] Commissioner for Human Rights, No space for violence against women and girls in the digital world. https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

[260] Panorama Global, (2023) I didn't consent: A Global Landscape Report on Image-Based Sexual Abuse, Prepared by: The Image-Based Sexual Abuse Initiative. https://assets-global.

website-files.com/62448c65f2a3dc7ae94193bd/63fe26f284d41703fac49b17_IBSA%20Landscape%20Report%202023%20by%20Panorama%20Global%20v20230228.pdf

[261] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[262] Article 4(1)(h) of the Romanian Domestic Violence Law (Law no.217/2003), as amended by Article I(2) of Law 106/2020. Law 106/2020 Completing and Modifying Law 217/2003 on Preventing And Fighting Domestic Violence.

[263] Commissioner for Human Rights, No space for violence against women and girls in the digital world. https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

[264] House of Commons Library, Online Safety Bill: progress of the Bill. https://commonslibrary.parliament.uk/research-briefings/cbp-9579/

[265] UK Governement, Cyberflashing, epilepsy-trolling and fake news to put online abusers behind bars from today https://www.gov.uk/government/news/cyberflashing-epilepsy-trolling-and-fake-news-to-put-online-abusers-behind-bars-from-today

[266] UNFPA, What makes TFGBV different from other forms of violence? https://www.unfpa.org/sites/default/files/resource-pdf/TFGBV_Brochure-1000x560.pdf

[267] Rigotti, C. and Al. (2023), Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. https://cris.vub.be/ws/portalfiles/portal/92354738/20322844221140713.pdf

[268] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[269] FRA (European Union Agency for Fundamental Rights) (2014), Violence against Women: An EU-wide survey – Main results report, Publications Office of the European Union, Luxembourg. https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

[270] Wheatcroft, J. et Al. (2017). Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses. SAGE Open.

[271] Glitch. (2020). The Ripple Effect: COVID-19 and the epidemic of online abuse.

[272] UN Women, 2023, Technology-facilitated Violence against Women: Taking stock of evidence and data collection.

[273] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[274] Equality Now (2021), Ending Online Sexual Exploitation and Abuse of Women and Girls.

[275] Ibid.

[276] Posetti, J. et Al. (2022), The Chilling: Assessing Big Tech's Response to Online Violence Against Women Journalists.

[277] UN Women, 2023, Technology-facilitated Violence against Women: Taking stock of evidence and data collection.

[278] World Economic Forum, Technology is changing faster than regulators can keep up - here's how to close the gap. https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/

[279] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[280] Ibid.

[281] Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform. https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae

[282] UNFPA (2023), Measuring technology-facilitated gender-based violence. A discussion paper.
[283] UN Women, 2023, Technology-facilitated Violence against Women: Taking stock of evidence and data collection.

[284] UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[285] Interviews with a representative of DG Connect and an independent researcher (see Annex II).

[286] Commissioner for Human Rights, No space for violence against women and girls in the digital world. https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

[287] Consultation with a representative of GREVIO (see Annex II).

[288] Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform. https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae

[289] Consultation with an expert on CVAW (see Annex II).

[290] GREVIO (2021), General Recommendation No 1 on the digital dimension of violence against women, Council of Europe, Strasbourg. https://rm.coe.int/%20grevio-rec-no-on-digital-violence-against-women/1680a49147

[291] Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform. https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae

[292] Cyberviolence, Challenges to the investigation and prosecution. https://www.coe.int/en/web/cyberviolence/challenges-to-the-investigation-and-prosecution

[293] Ibid.

[294] The Nordic Gender Equality Fund (2017), Online violence against women in the Nordic Countries. https://www.nikk.no/wp-content/uploads/Report-Online-Violence-Single-page-Web.pdf

[295] Ibid.

[296] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[297] Consultation with Silvia Semenzin, independent researcher (see Annex II).

[298] United Nations, 2022, Intensification of efforts to eliminate all forms of violence against women and girls, Report of the Secretary-General.

[299] Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform. https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae

[300] Panorama Global, (2023) I didn't consent: A Global Landscape Report on Image-Based Sexual Abuse, Prepared by: The Image-Based Sexual Abuse Initiative. https://assets-global.website-files.com/62448c65f2a3dc7ae94193bd/63fe26f284d41703fac49b17_IBSA%20Landscape%20Report%202023%20by%20Panorama%20Global%20v20230228.pdf

[301] Expert Opinion by Professor Clare McGlynn, Durham Law School, Durham University, UK and Professor Lorna Woods, School of Law, University of Essex, UK (2022), Image-Based Sexual Abuse, Pornography Platforms and the Digital Services Act. https://hateaid.org/wp-content/uploads/2022/04/ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf

[302] UN Women, Op-Ed: Tackling the hidden perils of technology-facilitated violence against women. https://eca.unwomen.org/en/stories/op-ed/2023/11/op-ed-tackling-the-hidden-perils-of-technology-facilitated-violence-against-women

[303] The Guardian, Inside the Taylor Swift deepfake scandal: 'It's men telling a powerful woman to get back in her box. Deepfake. https://www.theguardian.com/technology/2024/jan/31/inside-the-taylor-swift-deepfake-scandal-its-men-telling-a-powerful-woman-to-get-back-in-her-box

[304] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[305] Ibid.

[306] FRA (2023), Online Content Moderation – Cu-

rrent challenges in detecting hate speech, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-online-content-moderation_en.pdf

[307] Khoon, C. (2021) Deplatforming Misogyny. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[308] Expert Opinion by Professor Clare McGlynn, Durham Law School, Durham University, UK and Professor Lorna Woods, School of Law, University of Essex, UK (2022), Image-Based Sexual Abuse, Pornography Platforms and the Digital Services Act. https://hateaid.org/wp-content/uploads/2022/04/ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf

[309] The New York Times, Pornhub's Parent Company Admits to Profiting From Sex Trafficking, https://www.nytimes.com/2023/12/21/nyregion/pornhub-aylo-profits-sex-trafficking.html

[310] The Journal, Fake Porn, Real Victims: We must stop the easy use of AI to create nude images of women & girls. https://www.thejournal.ie/readme/online-safety-spain-artificial-intelligence-6182025-Oct2023/?utm_source=shortlink

[311] Hate Aid, Transparency reports: How social media platforms fail on users' rights, https://hateaid.org/en/transparency-reports-social-media-plattforms/

[312] Ibid.

[313] Council of Europe, The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform, https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae

[314] De Vido, S. and Sosa, L. (2021), Criminalisation of gender-based violence against women in European states, including ICT-facilitated violence, Publications Office of the European Union, Luxembourg

[315] Rigsadvokatmeddelelsen 'Digitale sexkrænkelser' issued on the 1 of July 2020 is available here in Danish: https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/870f993d-5cd4-4043-9d1d-30f4200d3132?showExact=true#37bb3a605b

[316] GREVIO(2019) Baseline Evaluation Report Portugal https://rm.coe.int/grevio-report-on-portugal/168091f16f

[317] Institut pour l'égalité des femmes et des hommes, Plainte au pénal contre Twitter pour la distribution non-consensuelle d'images intimes. https://igvm-iefh.belgium.be/fr/actualite/plainte_au_penal_contre_twitter_pour_la_distribution_non_consensuelle_dimages_intimes

[318] Chikane under valgkamp får lokalpolitikere til at trække sig: Partierne må på banen | Institut for Menneskerettigheder https://menneskeret.dk/nyheder/chikane-valgkamp-faar-lokalpolitikere-traekke-partierne-maa-paa-banen

[319] Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform.

[320] MenABLE, https://www.menable.eu/

[321] Naffi, N. et Al. (2023) Empowering Youth to Combat Malicious Deepfakes and Disinformation: An Experiential and Reflective Learning Experience Informed by Personal Construct Theory, Journal of Constructivist Psychology, https://www.tandfonline.com/doi/full/10.1080/10720537.2023.2294314

[322] Panorama Global, The Reclaim Coalition. https://www.panoramaglobal.org/reclaim

[323] INACH, #StopFisha. https://www.inach.net/stopfisha/#:~:text=-Created%20in%20April%202020%20during%20the%20quarantine%2C%20the,given%20to%20the%20practice%20of%20disseminating%20intimate%20content.

[324] #IAmHere Movement, https://iamhereinternational.com/about-us/

[325] Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform.

[326] StopNCII.org https://stopncii.org/about-us/

[327] Directive (EU) 2022/2381 of the European Parliament and of the Council of 23 November 2022 on improving the gender balance among directors of listed companies and related measures. https://eur-lex.europa.eu/eli/dir/2022/2381/oj

[328] UN Women (2023), The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[329] Information confirmed through interviews with Silvia Semenzin and Maria Joao Faustino (see Annex II).

[330] See EWL's position paper Towards a Europe Free from All Forms of Male Violence against Women (2010).

[331] Lobby Europeo de Mujeres en España (LEM España) (2024), Impact of Male Pornography Consumption on The Perpetration of Sexual Violence.

[332] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[333] Interview with Maria João Faustino, Post-Doctoral Researcher at the Center for Social Studies of the University of Coimbra, carried out on 18.03.2024 (see Annex II).

[334] EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[335] Rigotti, C. and Al. (2023), Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. https://journals.sagepub.com/doi/full/10.1177/20322844221140713

[336] Ibid.

[337] The consulted stakeholders agreed that the adoption of a new EU instrument specifically dedicated to CVAW is not necessary given that the Directive on VAW has recently been adopted. While an ad-hoc instrument could be regarded as more effective; on the other hand, it is important that offline and online violence are considered together within one instrument, as it has been done by the Directive.

[338] Report on extending the list of EU crimes to hate speech and hate crime 27.11.2023 - (2023/2068(INI)) https://www.europarl.europa.eu/doceo/document/A-9-2023-0377_EN.html

[339] A list of stakeholders consulted for this study is provided in Annex II.

[340] The importance of prevention was stressed by all consulted stakeholders (see annex II).

[341] Interview with Maria João Faustino, Post-Doctoral Researcher at the Center for Social Studies of the University of Coimbra, carried out on 18.03.2024. (see Annex II).

[342] European Women's Lobby (2023), Feminist Sexuality Education. https://www.womenlobby.org/IMG/pdf/lef_sexeduc_web.pdf

[343] The UN Broadband Commission, (2015), Cyber violence against women and girls https://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf

[344] Interview with Silvia Semenzin and Maria Joao Faustino (see Annex II).

[345] Commissioner for Human Rights, No space for violence against women and girls in the digital world. https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world