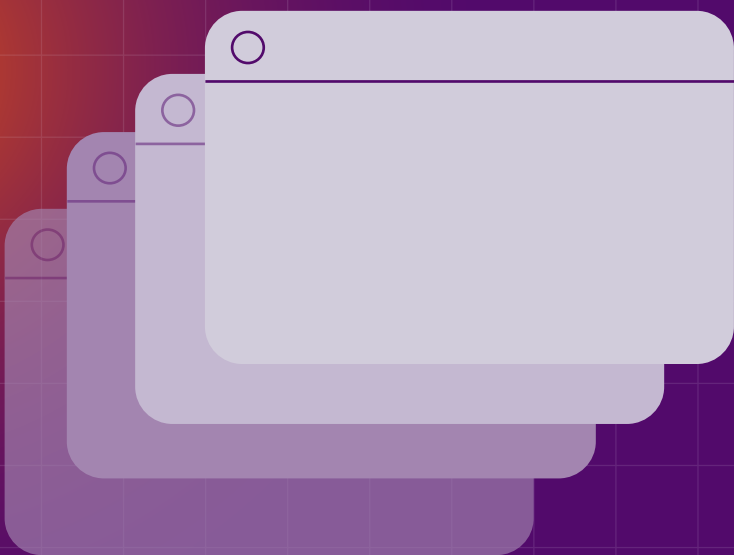
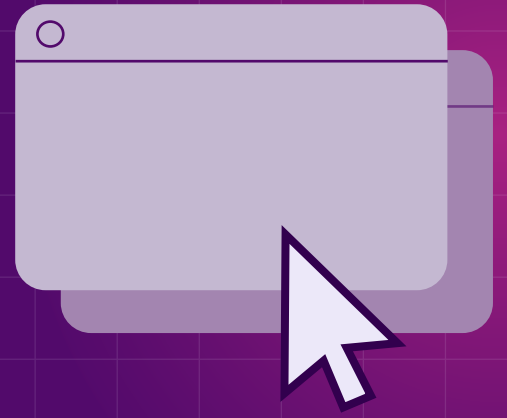


Report on Cyber Violence Against Women

EXECUTIVE SUMMARY
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

Maria João Faustino
Scientific Contribution

Iliana Balabanova
EWL President

Yvonne Redin
Graphic Design

Mary Collins
EWL Secretary General

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

Veronica Zaboia
Project Coordination

This Executive Summary has been translated in 25 languages plus an easy-to-read version to enhance its reach and impact. We thank EWL national coordinators and Soroptimist International of Europe members for the translations.



Funded by
the European Union



EUROPEAN WOMEN'S
LOBBY
EUROPEEN DES FEMMES

ACRONYMS

AI Artificial intelligence	EWL European Women’s Lobby	SDGs Sustainable Development Goals
CoE Council of Europe	EIGE European Institute for Gender Equality	TFV Technological- facilitated violence
CV Cyber violence	EPRS European Parliament Research Service	TF VAW Technological-facilitated violence against women
CVAWG Cyber violence against women and girls	FRA European Union Agency for fundamental rights	UN United Nations
CVAW Cyber violence against women	GBV Gender-based violence	VAW Violence against women
DV Domestic violence	GREVIO Group of Experts on Action against Violence against Women and Domestic Violence	VLOPs Very large online platforms
DSA Digital Service Act	ICT Information communication technology	VLOSEs Very large online search engines
DSC Digital service coordinator	IPV Intimate partner violence	VRD Victims’ Rights Directive
ECHR European Convention on Human Rights		

INTRODUCTION

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. 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. Data provided by EIGE¹ estimates that one in ten women have already experienced a form of cyber violence since the age of 15.

Seeking justice to combat online violence requires robust international legal and policy measures, as the virtual space knows no geographical boundaries. A holistic approach that encompasses legal tools to prevent cyber violence (CV) and effectively protect victims, accountability of technological (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.

This document is an executive summary of the European Women's Lobby's (EWL) 'Report on Cyberviolence against women: Policy Overview and Recommendations', available in 25 languages plus in an easy-to read version.

The 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.

AIM OF THE REPORT AND METHODOLOGICAL APPROACH

Following up on the 2017 [#HerNetHerRights report](#) & [Resource Pack](#),² this report aims to provide recommendations to policy makers and other stakeholders to counter cyber violence against women (CVAW).

The report has **five main objectives**:

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

The research underpinning this report took place over the period March-May 2024; the following research methods were used:

- **Desk research:** an in-depth 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/policy documents at EU, international and national level, was conducted to map legislative and policy instruments that may be applicable to CVAW.
- **Stakeholder consultation:** in order to further explore specific themes of the report, five key stakeholders from different categories (academia, institutions, NGOs) were consulted.



CYBER VIOLENCE AGAINST WOMEN (CVAW)

Cyber-violence (CV) is the use of online communication technologies to cause, facilitate or threaten violence against individuals.³

Definitions of CV vary considerably not only across countries but also across key actors in this field, with the result of having different terminologies and methodologies to measure it. Cyber violence against women (CVAW) **is a form of gender-based violence.**⁴ Evidence shows that CV has a clear gender dimension: women are more likely to experience unique forms of gendered violence in digital contexts, reflecting a similar pattern to violence against women (VAW) in the offline world.⁵ **CV is rooted in the same context of women's inequality as offline VAW.**⁶ Digital spaces reinforce and intensify **systemic structural gender inequalities** as well as patterns of harmful masculinities that drive all forms of VAW.⁷

In line with the Advisory Committee on Equal Opportunities for Women and Men,⁸ and according to the EWL, CV is part of a **continuum of VAW**; it does not exist in a vacuum, rather, it both stems from and sustains multiple forms

of offline violence.⁹ Indeed, online violence and offline violence are often interconnected and/or intertwined.¹⁰

Although CVAW is as harmful as offline violence, it has some specific features that distinguish it from other forms of VAW making it particularly dangerous. **It has a broad reach, transmission and speed**, which make it difficult to control the type of information that is disseminated via digital means. The **enhanced anonymity** offered by digital and virtual spaces allows users to behave with impunity. **It is hard to eliminate** and, thus, **re-traumatizing** for the victims.

Perpetrators of CVAW can be the victims' partners or ex-partners, family members, friends or anonymous individuals. **The impacts of CVAWG can be as serious as offline violence.**¹¹ Victims often withdraw from the digital sphere, silencing and isolating themselves and losing opportunities to build their education, professional career and support networks.¹²

MAIN FORMS OF CVAW

The report presents 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. The report acknowledges the fact that the forms of cyber violence are in continuum evolution, considering the fast evolving digital environment.

MOST PREVALENT FORMS

Data on the most prevalent forms of CV 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.¹³

INCREASINGLY THREATENING FORMS

Among the various forms, the **use of artificial intelligence (AI), virtual reality and online gaming** have become increasingly threatening to women. The use of AI has contributed to a sharp **increase in digital sexual forgeries (known as 'deepfakes')**.¹⁴ As reported by the EPRS' 2021 study, AI tools to create digital sexual forgeries are developing rapidly and are becoming cheaper, more sophisticated and accessible to users day by day.¹⁵ The World Economic Forum's Global Risks Report 2024¹⁶ has ranked

misinformation primarily driven by 'deepfakes', as the most severe global short-term risk the world faces in the next two years.

The gender dimension of the phenomenon is well evidenced. Sexual digital forgeries almost exclusively target women.¹⁷ Indeed, the majority of deepfake videos that are currently circulating online contain sexual images of women. **It has been estimated that between 90% and 95% of all 'deepfakes' concern material depicting nudity or sexually explicit activities;¹⁸ the vast majority of those 'deepfakes' (90%) concern women.**¹⁹

Similarly, 3D animation technology is increasingly able to generate videos with a similar quality to AI-based 'deepfake' technology.²⁰ Some deepfake programmes even combine AI image generation and 3D animation; most notably the **avatar technologies** that animate 3D models of a person's head or the entire body. The use of 3D avatars has spread in the metaverse where the **number of disturbing accounts of women being sexually assaulted and harassed by 3D avatars has increased.**²¹

Likewise, as more women join **online gaming communities**, they report experiencing high rates of sexual harassment online. Online gaming communities are perceived as one of the **most inequitable online environments for women.**²²

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.**

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 are those covered by the first ever European Directive on VAW adopted in April 2024: non-consensual sharing of intimate or manipulated material; cyber stalking; cyber harassment and cyber incitement to violence or hatred.

ADDITIONAL FORMS

The report provides a description of additional forms of CV (e.g. google bombing, sealioning* etc.). The list is non-exhaustive given that new forms continue to emerge with the increase in digitalization and the rapid evolution of technology. Among these additional forms, the 'manosphere' and pornography are described.

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.²³ **Pornography** promotes damaging stereotypes in its portrayal of women.

The production and sale of pornography entails and encourages VAW and plays a key role in shaping men's and women's conceptions of relationships. Besides, pornography makes violence 'sexy'. Figures show that the states with higher circulation rates of pornographic magazines have higher rape rates.²⁴

* 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.

PREVALENCE

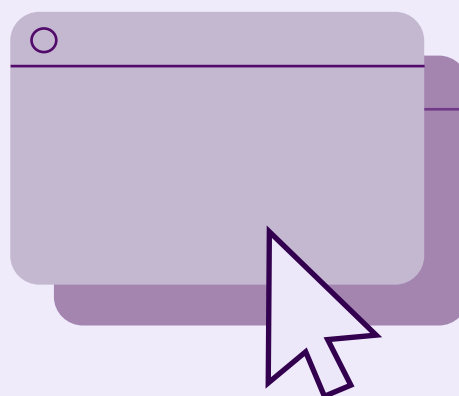
The **lack of agreed definitions of CV and methodologies for its measurement make it particularly difficult to assess the extent of the problem.**²⁵ Despite gaps and differences in methodologies, **some attempts to measure CV have been made at both international and EU level.**

At **international level**, a global report²⁶ which synthesised results from surveys on online VAWG, from 2018 onwards, estimated that between 16-58 % of women have experienced CVAW. 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.²⁷

The severe lack of data and research on CVAW is a major issue also at EU level. Some attempts to capture the prevalence of some forms of CVAW have been made by the Fundamental Rights Agency (FRA) back in 2014 and 2019.²⁸ The 2019 FRA's survey²⁹ 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.³⁰ 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 (18-35 years) 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.³¹

At **national level**, 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.³² In France, more than 4 out of 10 people say that they have been victims of cyber harassment.³³



THE GENDER DIMENSION OF CV

Cyber violence has a gender dimension. According to a 2023 FRA's report³⁴ focusing on online hate in social media posts, **women face more online harassment than any other target groups** (people of African descent, Jews and Roma). Similarly, an American study found that 33% of women under 35 report having been sexually harassed online, compared to 11% of men.³⁵ Along the same lines, GREVIO³⁶ 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.

While all women that have access to digital spaces are exposed to risks of CV, **some groups of women are particularly vulnerable.** 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, age**, among others.³⁷ **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.**³⁸

PERPETRATORS

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.**³⁹ For example, the vast majority of perpetrators of image-based sexual abuse are men.⁴⁰

Perpetrators can be one or a multitude. Given the fact that technology allows the easy and

fast dissemination of harmful content, 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).⁴¹



THE IMPACTS OF CVAW ON WOMEN

CVAW 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 CVAW as well as the interconnections between online and offline violence, make survivors feel in constant fear and insecurity.**⁴²

GREVIO refers to **severe psychological, economic and social impacts of CVAW.** 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. 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.⁴³

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.⁴⁴ 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.⁴⁵ The results is that CVAW limits women's public participation and leadership; **women's voices are silenced, discredited, and censored.**

LEGAL AND POLICY FRAMEWORK ON CVAW

INTERNATIONAL LEVEL

At **international level**, the United Nations (UN) and the Council of Europe (CoE) have addressed CVAW. The main legal instrument is the Council of Europe Convention on preventing and combating violence against women and domestic violence (**Istanbul Convention**).⁴⁶ The EU acceded to 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 2023.⁴⁷ Despite the EU's ratification, five EU Member States⁴⁸ have not yet ratified it.

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. The Convention shall be interpreted in light of the **GREVIO's General Recommendation n.1**⁴⁹ which categorises manifestations of VAW in the digital sphere as expressions of gender-based violence (GBV) covered by the Istanbul Convention.

EU LEVEL

At **EU level**, the main legislative instrument is the **Directive 2024/1385 on combating violence against women and domestic violence**,⁵⁰ adopted by the EU Parliament and the EU Council in April 2024. The latter 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 Directive also sets out the rights of victims of all forms of VAW or DV and provides for their protection.⁵¹

The Directive can be considered **as a significant step forward to better protect women and girls from VAW. It marks a significant improvement** in seeking to introduce minimum rules regarding these forms of CV.⁵² Among its strengths, the Directive encompasses in **just one instrument** both offline forms of VAW and online forms. 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.

Despite its strengths, the **Directive is not without limits and has been subject to criticism**. For example, Articles 5-8 on CVAW, refer to **intentional conducts**. This reference poses some legal challenges given that the intentionality of the act must be proved. It **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 information and communication technology (ICT) skills.

Moreover, Articles 5, 6 and 7 refer to **'serious harm'**. This condition creates legal uncertainty for victims across and within countries leaving to judicial discretion the decision on whether these conducts are punishable. This formulation is based on a lack of awareness on the harmfulness of CV.⁵³

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 the EWL.⁵⁴

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.** Plus what might constitute 'sexual activities' is likely to vary considerably across Member States and give rise to definitional confusion.

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.⁵⁵

The **prompt removal of harmful material** is foreseen in Article 23 of the Directive on VAWG and DV; such measure complements action under another key instrument in the digital area, the **Digital Services Act**⁵⁶ (DSA). The latter, adopted in October 2022, aims to create a safer online environment for consumers and companies in the EU. It defines clear responsibilities for online platforms and social media; deals with illegal content and products, hate speech and disinformation; as well as increases transparency with better reporting and oversight.

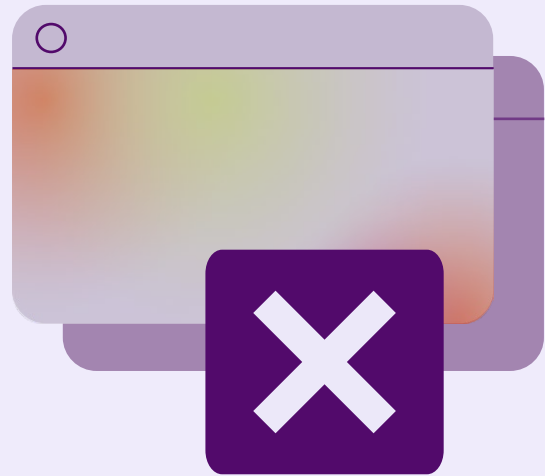
According to academics,⁵⁷ the measures in the **DSA can be considered a welcome recognition of the prevalence and harms of image-based sexual abuse. GBV is recognized as one of the macro area of risks** along with other risks. Within the macro area of GBV, **specific categories**⁵⁸ **are now in the process of being created by the Commission under the 'Transparency Reporting Package'**.

Another positive development under the DSA is the fact that the **Commission designated under the DSA three porn platforms (Pornhub, XVideos and Stripchat) as Very Large Online Platforms (VLOPs)** in December 2023.⁵⁹ The designation comes with heightened responsibilities regarding transparency and child protection.

OTHER RELEVANT EU LEGAL INSTRUMENTS APPLICABLE TO CVAW ARE:

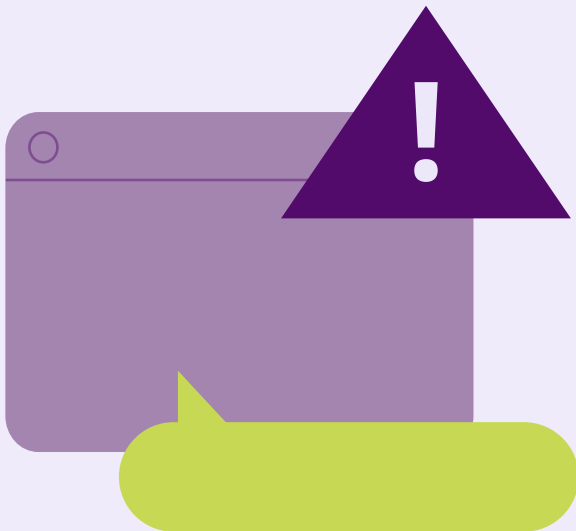
- The **Artificial Intelligence Act⁶⁰ (AI Act)**, adopted by the European Parliament on 13 March 2024. While the Act represents an opportunity to mitigate some of the risks posed by the misuse of AI such as ‘deepfakes’, it does not contain any express reference to CVAW. Moreover, the Act refers to gender equality only generically.⁶¹

- The **Victim’s Rights Directive⁶²** (Directive 2012/29/EU), still under revision as of 2024, which states that all victims of crime (including CV) 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.



- The **Directive on preventing and combating trafficking in human beings and protecting its victims⁶³** (Directive 2011/36/EU)⁶⁴ which was updated in April 2024. The revised version introduces trafficking in human beings committed or facilitated through ICTs, including internet and social media, as an aggravating circumstance when it relates to sexual exploitation.

- The **General Data Protection Regulation⁶⁵** (Regulation (EU) 2016/679) 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.⁶⁶



The Directive can be considered as a **significant step forward to better protect women and girls from VAW.**

NATIONAL LEVEL

Some Member States have taken important steps to prevent and combat certain aspects of CVAW in the last five years.⁶⁷ 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.

While **Italy** introduced a new criminal offence, the unlawful dissemination of sexually explicit images or videos, **Austria** adopted an online hate speech package which provides new tools to address this. 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 Offences criminalises all forms of non-consensual sharing of intimate images, with penalties of 10 years in prison.⁶⁸

Outside the EU, the **UK has recently adopted new initiatives to criminalise cyberflashing and more generally illegal content online** through the Online Safety Act, which gained Royal Assent in 2023.⁶⁹

KEY CHALLENGES

The following challenges have been identified:

- The **lack of awareness and the underestimation** of the seriousness of CVAW are major issues that contribute to the **under-reporting** of incidents.
- At international and EU level, there is **not yet a harmonised definition of CVAW**. As a result, **legal and statistical definitions of CV vary greatly** across countries and organisations. Moreover, most definitions are **gender-neutral and do not acknowledge the links between online and offline violence**.
- Considering the rapid evolution of technology, **legal frameworks on CVAW tend to become outdated very quickly**.
- The **lack of data on CVAW** 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.
- The **under-representation of women in the ICT sector contributes to the lack of a gender dimension into ICT products** including online gaming and virtual reality platforms, where CVAW is increasing.
- 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**.
- **Social media and online platforms do not always act effectively** to remove illegal and harmful content. **Complaint reporting systems** of online platforms are not always user-friendly, with the result that victims do not know to whom they can ask support.



GOOD PRACTICES TO TACKLE CVAW

Good practices of different types have been identified within and outside the EU; the latter have been categorised based on their scope and focus. One example for each practice is provided below:

▶ **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 how to deal with cases of CVAW was also adopted and distributed to all Slovenian police stations and directorates, prosecutors' offices and courts.⁷⁰

▶ **Involvement of national human rights institutions:** National human rights institutions play an important role in combating CVAW, particularly when their mandate allows them to investigate cases of online hate speech. In Belgium, the Institute for Equality between Women and Men filed a criminal complaint against a social media platform for refusing to take down non-consensual intimate images.⁷¹

▶ **Prevention:** A study,⁷² 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' and explored their capacity and willingness to effectively counterbalance disinformation.

▶ **Survivors' involvement:** The Reclaim Coalition to End Online Image-based Sexual Violence⁷³ 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.

▶ **Helplines:** Access Now Digital Security Helpline helps women at risk of CV 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.

▶ **Countering cyber-sexism and online hate speech:** #StopFisha⁷⁴ is a French feminist

NGO which aims to fight cyber-sexism. It was created as a support for victims and as an alert to denounce cyber-sexism during the covid-19 pandemic. As the movement continued growing, #StopFisha became an NGO which now tackles all forms of sexist and sexual cyberviolence.

► **Specialised support services:** 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.⁷⁵

► **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.⁷⁶



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.

GENERAL RECOMMENDATIONS

Empower survivors: 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. Survivors often experience victim 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: It is paramount 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.

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 CVAW through key partnerships and coordinated actions would avoid the current overlaps and gaps in actions. Ongoing exchanges of knowledge and cooperation among key actors are essential, including learning from countries with more advanced systems for addressing CVAW.

Ensure that the technology sector, in particular social media and online platforms, meet their obligations: Social media and online platforms must be held accountable in the fight against CVAW. 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. Moreover, they should provide effective resources for users to recognize and intervene against online abuse. In brief, increased transparency and accountability, faster removal of illegal content, safety by design and prevention are needed from tech companies, online platforms and social media, including porn platforms.

Approach pornography in the continuum of VAW: The EWL denounces the business of pornography and highlights the enormous financial profits made by pornography industries, in complicity with prostitution businesses. The EWL advocates for the EU and Member States to take action to ensure that pornography is recognised as a form of VAW.

RECOMMENDATIONS FOR 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. To date, the only attempt to harmonise legal and statistical definitions of CVAW has been carried out by EIGE.⁷⁷ EIGE's definitions should be adopted by all EU institutions.

Develop guidelines and indicators for data collection on CVAW: the EU should develop clear guidelines and indicators supporting Member

States in their efforts to collect data on CVAW, as currently done by EIGE.

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, 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. 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. The 2008 Framework Decision on combating certain forms and expressions of racism and xenophobia should also be revised to incorporate reference to gender hate speech by ICT means.

Effectively enforce the DSA: 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

Overall, a cultural systemic change is required to tackle CVAW from a gender and an intersectional perspective and as a continuum of violence.

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.

Incorporate reference to CVAW under the Artificial Intelligence Act: In light of the proliferation of sexual digital forgeries ('deepfakes') and other forms of VAW through AI, it is urgently recommended that future updates of the AI Act address CV through a comprehensive gender-sensitive approach.

Issue regular guidance on new forms of CVAW: Given the rise in forms of CVAW facilitated by artificial intelligence and the incapacity of legal/policy frameworks to keep at pace with new ICT developments, the EU should issue regularly a guidance on how to tackle the latest forms of CVAW in an effective way.

RECOMMENDATIONS FOR MEMBER STATES

Align national definitions of CVAW with harmonised gender-sensitive EU definitions: Member States should incorporate EU har-

monised 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.

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.

Ratify and implement the Istanbul 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.

Strengthen prevention in the broad sense: It is paramount to tackle gender stereotypes and social norms of inequality at the broader societal level including through the empowerment of

women. 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 programmes from an early age for both boys and girls.⁷⁸ Moreover, as recommended by the EWL in its report,⁷⁹ implement mandatory, relationship and sexuality education from a feminist perspective is paramount. Educating men and boys on the forms, severity and consequences of CVAW is also crucial. Overall, a cultural systemic change is required to tackle CVAW from a gender and an intersectional perspective and as a continuum of violence.

Criminalise CVAW in line with the Directive on VAW: It is recommended that Member States criminalise the main forms of CVAW in line with Articles 5 to 8 of the Directive on VAW and keep the legislation abreast of technology developments. 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: It is essential that National Digital Service Coordinators 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.

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 trans-border acts of CV. The effective enforcement of the legal framework on CVAW is crucial.

Improve victims' access to remedies: It is important to guarantee easily accessible and safe reporting mechanisms both online and off-line, enabling women to report CV. Information on legal avenues and other remedies should be made easily accessible to victims of CVAW.

Provide specialised support services: It is 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 to equip them with knowledge on digital expressions of VAW, that would enable them to respond to women without causing secondary victimisation and re-traumatisation.

ENDNOTES

¹EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

²European 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>

³European Parliament Research Service (EPRS) (2021), Combating Gender based Violence: Cyber Violence. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2021\)662621](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621)

⁴EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

⁵UN 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>

⁶Ibid

⁷World Wide Web Foundation (2021), Online Gender-Based Violence and Abuse: Consultation Briefing. <https://uploads-ssl.webflow.com/>

[61557f76c8a63ae527a819e6/61_5585a9bb-feb883](https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en)
[6d512947_OGBV_ConsultationBriefing.pdf](https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en)

⁸European Commission, Advisory Committee on Equal Opportunities for Women and Men (2020), Opinion on combatting online violence against women, Brussels. https://commission.europa.eu/document/download/eae53eb9-ca88-4fc0-8a6e-51e771c96f68_en?filename=opinion_online_violence_against_women_2020_en.pdf

⁹Professor Liz Kelly was the first to establish the concept of a ‘continuum of violence’ in her book ‘Surviving Sexual Violence’ (1st ed.)(1988). Polity.

¹⁰European Parliament Research Service (EPRS) (2021), Combating Gender based Violence: Cyber Violence. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2021\)662621](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621)

¹¹UN 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>

¹²Ibid

¹³The Economist Intelligence Unit (2021), Measuring the Prevalence of Online Violence against Women. <https://onlineviolencewomen.org/>

[eiu.com/](https://www.eiu.com/). A survey was conducted across 45 countries (a sample of 100 replies for each country).

¹⁴The term 'deepfakes' is a fusion 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. 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 term 'sexual digital forgeries' as suggested by Mary Anne Franks, professor at George Washington University Law School and President and Legislative & Tech Policy Director of the Cyber Civil Rights Initiative, a nonprofit organisation dedicated to combating online abuse and discrimination. 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' under brackets.

¹⁵European Parliament Research Service (EPRS) (2021), Tackling deepfakes in European policy. The study refers to 'Non-consensual pornographic deepfakes', however, the EWL prefers to use the term 'sexual digital forgeries'. [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU\(2021\)690039_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf)

¹⁶World Economic Forum (2024), The Global Risk Report 2024. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

¹⁷Ibid. The EPRS (2021) study refers to 'Non-consensual pornographic deepfakes'.

¹⁸Patrini, Georgio (2019), Mapping the Deepfake Landscape. Sensity. The report refers to 'material depicting pornography', however the EWL prefers to refer to 'material depicting nudity or sexually explicit activities'. <https://giorgiop.github.io/posts/2018/03/17/mapping-the-deep-fake-landscape/>

¹⁹Ibid.

²⁰European 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](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf)

²¹Monash Lens (2022), Sexual assault in the metaverse is part of a bigger problem. <https://lens.monash.edu/@politics-society/2022/07/22/1384871/sexual-assault-in-the-metaverse-theres-nothing-virtual-about-it>

²²Information provided by a representative of DG Connect (interview carried out on 16.02.2024).

²³Rothermel, A.-K. (2023), The role of evidence-based misogyny in antifeminist online communities of the 'manosphere'. *Big Data & Society*, 10(1). <https://journals.sagepub.com/doi/10.1177/20539517221145671>

²⁴Baron & Straus (1984), in Mary Anne Layden. *Pornography and Violence: a new look at research*, 2009. https://www.socialcostsofpornography.com/Layden_Pornography_and_Violence.pdf

²⁵UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwomen.org/sites/default/files/2022-10/Accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls-en_0.pdf

²⁶Hicks, J. (2021), Global evidence on the prevalence and impact of online gender-based violence (OGBV).

²⁷The 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). https://opendocs.ids.ac.uk/articles/report/Global_Evidence_on_the_Prevalence_and_Impact_of_Online_Gender-based_Violence_OGBV_/26428096?file=48181987

²⁸FRA (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>

²⁹FRA (2021), 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

³⁰HateAid (2021), Boundless hate on the internet – Dramatic situation across Europe. https://hateaid.org/wp-content/uploads/2022/04/HateAid-Report-2021_EN.pdf

³¹Ibid

³²Bumble (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>

³³Ipsos (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>

³⁴FRA (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

³⁵Pew Research Centre, (2021), The state of online harassment. <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>

³⁶GREVIO (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>

³⁷The 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>

³⁸UNESCO (2020), Online violence against women journalists: a global snapshot of incidence and impacts. <https://unesdoc.unesco.org/ark:/48223/pf0000375136>

³⁹Ibid.

⁴⁰Henry, N., McGlynn, C. et. Al (2020), Image-based Sexual Abuse, A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery. <https://www.routledge.com/Image-based-Sexual-Abuse-A-Study-on-the-Causes-and-Consequences-of-Non-consensual-Nude-or-Sexual-Imagery/Henry-McGlynn-Flynn-Johnson-Powell-Scott/p/book/9780367524401>

⁴¹UN 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>

⁴²United Nations Population Fund (UNFPA) (2021), Making all spaces safe Technology-facilitated Gender-based Violence. <https://www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe>

⁴³Ibid.

⁴⁴The 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

⁴⁵Posetti, 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>

⁴⁶Council of Europe, 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>

⁴⁷European Parliament (2023), EU accession to the Istanbul Convention, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739323/EPRS_ATA\(2023\)739323_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739323/EPRS_ATA(2023)739323_EN.pdf)

⁴⁸Bulgaria, Czechia, Hungary, Lithuania and Slovakia.

⁴⁹GREVIO (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>

⁵⁰EU Directive 2024/1385 on combating violence against women and domestic violence. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401385

⁵¹Council of the European Union (2024), Violence against women: Council and European Parliament reach deal on EU law. <https://www.consilium.europa.eu/en/press/press-releases/2024/02/06/violence-against-women-council-and-european-parliament-reach-deal-on-eu-law/>

⁵²Rigotti, 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>

⁵³EWL (2023), 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>

⁵⁴Ibid.

⁵⁵Ibid.

⁵⁶Regulation (EU) 2022/2065 of the European Parliament and of the Council of 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/>

⁵⁷Professor Clare McGlynn (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>

⁵⁸These 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.

⁵⁹European Commission (2023), 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-actTXT/?toc=OJ%3AL%3A2022%3A277%3ATOC&uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG

⁶⁰Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

⁶¹Interview with a representative of DG Connect carried out on 16.02.2024.

⁶²Directive 2012/29/EU 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>

⁶³Directive 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>

⁶⁴Ibid.

⁶⁵Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

⁶⁶EIGE (European Institute for Gender Equality) (2022), Combating cyber violence against women and girls, Vilnius.

⁶⁷Council of Europe (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>

⁶⁸Panorama 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>

⁶⁹UK Parliament, House of Commons Library, Online Safety Bill: progress of the Bill. <https://commonslibrary.parliament.uk/research-briefings/cbp-9579/>

⁷⁰Council 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>

⁷¹Institut pour l'égalité des femmes et des hommes, 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_

⁷²Naffi, 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>

⁷³Panorama Global, The Reclaim Coalition. Last accessed in May 2024. <https://www.panoramaglobal.org/reclaim>

⁷⁴Inach, #StopFisha. Last accessed in May 2024. <https://www.inach.net/stopfisha/#::~:~:text=Created%20in%20April%202020%20during%20the%20quarantine%2C%20the,given%20to%20the%20practice%20of%20disseminating%20intimate%20content.>

⁷⁵Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform. <https://www.coe.int/en/web/istanbul-convention/edvaw-platform>

⁷⁶StopNCII, About us. Last accessed in May 2024. <https://stopncii.org/about-us/>

⁷⁷EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

⁷⁸The importance of prevention was stressed by all consulted stakeholders (see Annex II of the full report).

⁷⁹EWL (2020), Feminist Sexuality Education. https://www.womenlobby.org/IMG/pdf/lef_sexeduc_web.pdf