1. What is cyber violence against women and girls?

Digital platforms have often been celebrated for allowing equal opportunities for public self-expression, regardless of one’s identity and status. Yet, not everyone is welcome in the cyberspace. The digital arena has become a breeding ground for a range of exclusionary and violent discourses and beliefs, expressed and disseminated in a context of anonymity and impunity.

Both women and men can be victims of cyber violence. However, evidence shows that women and girls are highly exposed to it. Not only are they more likely to be targeted by cyber violence, but they can suffer from serious consequences, resulting in physical, sexual, psychological, or economic harm and suffering.

Cyber violence against women and girls (CVAWG) is often dismissed as an insignificant and virtual phenomenon. However, CVAWG does not exist in a vacuum: it is an act of gender-based violence that is perpetrated through new technologies, but is deeply rooted in the inequality between women and men that still persists in our societies.

What are the main features of CVAWG?

- Many different forms of CVAWG exist. Many could be seen as online extensions of forms of violence perpetrated in the physical world (such as cyber harassment or cyber stalking). However, the cybersphere also leads to different and unique forms of violence (such as non-consensual intimate image abuse or doxing) and can amplify the scale of harm compared to violence perpetrated in the physical world.

- CVAWG is perpetrated across different cyberspaces, including social media platforms, messaging apps and discussion sites. As the digital environment is constantly evolving, new technologies are bound to give rise to new and diverse manifestations of violence. For example, the Metaverse is emerging as a new space for the perpetration of virtual rape and other forms of CVAWG.

- A vast array of information and communications technology (ICT) tools may be misused to stalk, harass, survey and control victims, including smartphones, computers, cameras, and other recording equipment. If we consider the broader understanding of technology-facilitated violence, available tools encompass the whole Internet of Things (IoT) and include: GPS or satellite navigators, smart watches, fitness trackers and smart home devices, as well as dedicated digital technologies like spyware and stalkerware.

- Different types of perpetrators exist, including those commonly considered in a gender-based violence context, such as relatives, acquaintances, intimate partners, and ex-partners. However, perpetrators can also be anonymous and/or unacquainted in the cybersphere.

- CVAWG is a cross-cultural, global phenomenon. The global networking features of social media platforms allow frequent spillover phenomena: new online communities are formed across national borders with the shared aim of hating women and girls, such as the so-called ‘Manosphere’ and the ‘Incel’ community.

---

How is ‘online’ violence connected to ‘offline’ violence and vice versa?

Digital acts of violence do not always lead directly to physical harm, which is traditionally regarded as the most ‘visible’ and ‘indisputable’ form of violence. As a result, CVAWG is often quickly dismissed as an insignificant, virtual phenomenon that is less impactful and harmful to its victims.

In reality, digital (online) and physical (offline) spaces are more and more integrated and experienced as a single, enmeshed reality. As mentioned in a study requested by the European Parliament’s FEMM Committee, CVAWG often reflects (or is a precursor for) forms of abuse and victimisation in the physical world, carried out and/or amplified through digital means.

A European Parliamentary Research Service study has recently quantified the cost of gender-based cyber violence to be in the order of €49.0 to €89.3 billion. Tangible economic costs include legal or healthcare assistance, the latter related to an increased incidence of mental health issues, like depression and anxiety disorders. The largest cost category was the monetised value of the loss in terms of quality of life, accounting for about 60% for cyber harassment and about 50% for cyber stalking.

CVAWG can intensify in times of crisis. Evidence suggests that the lockdowns and social distancing measures mandated to reduce the spread of COVID-19 were associated with a spike in digital forms of violence affecting women and girls specifically, such as cyber harassment and non-consensual intimate image abuse.

How is cyber violence gendered?

CVAWG is part of the continuum of violence against women and girls and represents yet another form of abuse and silencing embedded within existing gendered power structures. The violent acts taking place through technology are an integral part of the same violence that women and girls experience in the physical world, for reasons related to their gender.

Also, there are many forms of cyber violence that target women and girls almost exclusively. These include forms of non-consensual intimate image abuse, like cyber flashing and sextortion as well as virtual rape.

An EIGE study on Gender Equality and Digitalisation in the European Union highlighted the new gendered challenges of digitalisation, including women being potential targets of CVAWG from a very young age. Often resulting in an abandonment of digital spaces, CVAWG has a devastating impact on women’s confidence when it comes to technology, further contributing to worsening gender equality issues like STEM/ICT gender segregation and gender pay gap.
Which groups of women and girls are particularly vulnerable to CVAWG?

CVAWG is an intersectional form of violence with different patterns and levels of vulnerability and risk for specific groups of women and girls.

In a 2014 FRA survey conducted across the 28 Member States of the European Union (EU), 34% of the respondents with disabilities had experienced physical, sexual, or psychological violence and threats of violence (including online), compared with 19% of women who did not have a disability.

Among migrants, second generations and ethnic or religious minorities, cyber violence can lead to lower trust in institutions and ultimately damage social integration.

As mentioned in a 2021 European added value assessment study, CVAWG can be stronger towards lesbian, bisexual and transgender women, as well as women from racial minority groups and different religious communities.

What are the key challenges to tackle CVAWG across the EU?

Despite the prevalence of the phenomenon, CVAWG remains under-reported in the EU and there is a significant lack of comprehensive and comparable data.

Victims do not always believe that their cases will be taken seriously by law enforcement and, consequently, decide not to report. Even in anonymous surveys, respondents may not be aware that their experiences can be considered as cyber violence. Under-reporting contributes to a lack of data and obscures the true scale and prevalence of the problem.

Another challenge is linked to the great variety of legal and statistical definitions of cyber violence across Member States (MS). Even in the same MS, definitions tend to overlap and the distinction between different forms of cyber violence becomes blurred. The absence of harmonized and mutually exclusive definitions is also directly related to the severe lack of good quality data.

The variety of overlapping definitions is also related to the fact that general offences apply in the majority of CVAWG cases at MS level. For example, stalking and harassment would apply instead of specific offences targeting the unique characteristics and consequences of cyber stalking and cyber harassment.

Moreover, existing definitions do not take into account the continuum of violence between physical and digital spaces, tend to be gender neutral and overlook the intersectional patterns of vulnerability and risk for specific groups of women and girls.

---

2. EIGE’s definitions of cyber violence against women and girls

Cyber violence against women and girls

Cyber violence against women and girls includes a range of different forms of violence perpetrated by ICT means on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or personal beliefs).

All acts of CVAWG can:

a) start online and continue offline such as in the workplace, at school or at home;
b) start offline and continue online across different platforms such as social media, emails or instant messaging apps;
c) be perpetrated by a person or group of people who are anonymous and/or unknown to the victim;
d) be perpetrated by a person or group of people who are known to the victim such as an (ex) intimate partner, a school mate or co-worker.

Cyber stalking against women and girls

Cyber stalking against women and girls involves intentional repeated acts against women and/or girls because of their gender, or because of a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or beliefs).

It is committed through the use of ICT means, to harass, intimidate, persecute, spy or establish unwanted communication or contact, engaging in harmful behaviours that make the victim feel threatened, distressed or unsafe in any way.

- Cyber stalking is a key tactic of coercive control used in intimate partner violence (IPV). 7 in 10 women who have experienced cyber stalking have also experienced at least one form of physical and/or sexual violence from an intimate partner.\(^\text{10}\)

- Several studies highlight the links between stalking and cyber stalking\(^\text{11}\): a UK study found that over half (54%) of cyber stalking cases involved a first encounter in the physical world\(^\text{12}\). Also, obtaining personal information through cyber stalking can lead to further violent actions both online and offline\(^\text{13}\).

- The negative impact of cyber stalking on the victims’ well-being appears similar to that of stalking\(^\text{14}\). Cyber stalking victims report increased suicidal ideation, fear, anger, depression, and post-traumatic stress disorder symptomology\(^\text{15}\).


Cyber harassment against women and girls

Cyber harassment against women and girls involves one or more acts against victims because of their gender, or because of a combination of gender and other factors (e.g. race, age, disability, profession, personal beliefs or sexual orientation).

It is committed through the use of ICT means to harass, impose or intercept communication, with the purpose or effect of creating an intimidating, hostile, degrading, humiliating or offensive environment for the victim.

- According to a 2019 FRA survey, 13% of women across the EU, the UK and North Macedonia had experienced cyber harassment during the previous 5 years. Victims are more commonly younger respondents (20% of young women aged 18 to 29), members of the LGBTIQ+ community and people with disabilities.

- Cyber harassment tends to reflect a broader pattern of victimization on the offline-online continuum of violence. 77% of women who have experienced cyber harassment have also experienced at least one form of sexual and/or physical violence perpetrated by an intimate partner.

- 41% of responding women who experienced cyber harassment felt that their physical safety was threatened. One in two women have experienced reduced self-esteem or loss of self-confidence, stress, anxiety, or panic attacks because of cyber harassment.

Cyber bullying against girls

Cyber bullying against girls means any form of pressure, aggression, harassment, blackmail, insult, denigration, defamation, identity theft or illicit acquisition, treatment or dissemination of personal data, carried out repeatedly by ICT means on the grounds of gender or a combination of gender and other factors (e.g. race, disability or sexual orientation), whose purpose is to isolate, attack or mock a minor or group of minors.

- There is a strong connection between cyber bullying and bullying: most students who are victims of cyber bullying have been bullied in school first, and a large percentage of victims of cyber bullying have been bullied both online and offline, often by the same perpetrator(s).

- Across the OECD countries with available data, about 12% of girls aged 15 report having been cyber bullied, compared with 8% of boys. The Cyberbullying Research Center found that adolescent girls are more likely than boys (50.9% vs. 37.8%) to have experienced cyber bullying in their lifetimes.

- Certain minority groups are more exposed to cyber bullying, such as LGBTIQ+ individuals and students with special needs. Also, there are clear links between cyber bullying and mental health problems.

---


20 OECD (Organisation for Economic Co-operation and Development) (2019), 'Girls are more exposed than boys to cyberbullying' (https://www.oecd.org/gender/data/girls-are-more-exposed-than-boys-to-cyberbullying.htm).


Online gender-based hate speech

Online gender-based hate speech is defined as content posted and shared through ICT means that:

a) is hateful towards women and/or girls because of their gender, or because of a combination of gender and other factors (e.g. race, age, disability, sexuality, ethnicity, nationality, religion or profession); and/or

b) spreads, incites, promotes or justifies hatred based on gender, or because of a combination of gender and other factors (e.g. race, age, disability, sexuality, ethnicity, nationality, religion or profession).

It can also involve posting and sharing, through ICT means, violent content that consists of portraying women and girls as sexual objects or targets of violence.

This content can be sent privately or publicly and is often targeted at women in public-facing roles.

Non-consensual intimate image abuse

Non-consensual intimate image (NCII) abuse against women and girls involves the distribution through ICT means or the threat of distribution through ICT means of intimate, private and/or manipulated images/videos of a woman or girl without the consent of the subject.

Images/videos can be obtained non-consensually, manipulated non-consensually, or obtained consensually but distributed non-consensually. Common motivations include sexualizing the victim, inflicting harm on the victim, or negatively affecting the life of the victim.

- Victims may decide to post less often, tone down their language to mitigate provocation or even deactivate their accounts. According to Amnesty International, this self-censorship has a ‘silencing effect’ and results in women and girls not openly participating to debates and meaningful exchanges online.

- As victims are often prominent female figures like politicians, journalists or sportswomen, online gender-based hate speech directly impacts on the presence and activities of potential role models for girls who may want to pursue careers in traditionally male-dominated industries.

- ICT means can contribute to make online forms of gender-based hate speech more harmful, because it is significantly more difficult to permanently remove abusive or triggering content from the Internet, which often results in re-victimisation.


3. Glossary of terminology related to CVAWG²⁸

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber Flashing</strong></td>
<td>Sending unsolicited sexual images using dating apps, message apps or texts, or using Airdrop or Bluetooth. Cyber flashing is a form of non-consensual intimate image (NCII) abuse.</td>
</tr>
<tr>
<td><strong>Deepfake</strong></td>
<td>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. Most deepfakes of women and girls depict intimate pictures or sexual activities and are shared on platforms/adult entertainment websites, without consent to their creation and publication. Deepfake is a form of non-consensual intimate image (NCII) abuse.</td>
</tr>
<tr>
<td><strong>Digital Voyeurism</strong></td>
<td>An umbrella term for different forms of non-consensual intimate image (NCII) abuse. It refers to the surreptitious and non-consensual filming of an unsuspecting woman’s cleavage, thighs, or genitalia (see downblousing, upskirting) in public or private places. These photos are also known as creepshots. Digital voyeurism can also refer to perpetrators sending unsolicited sexual images (often of their own private parts), such as cyber flashing.</td>
</tr>
<tr>
<td><strong>Downblousing</strong></td>
<td>Surreptitious and non-consensual filming of an unsuspecting woman’s cleavage in public or private places. Downblousing pictures or videos are usually published, traded, and exchanged on the internet without the victim’s knowledge. Downblousing is a form of non-consensual intimate image (NCII) abuse.</td>
</tr>
<tr>
<td><strong>Doxing</strong></td>
<td>Researching, manipulating, and publishing private information about an individual, without their consent as to expose and shame the victim. As information usually allows victims to be physically located, doxing can also be a precursor for violence in the physical world. Doxing is often perpetrated in the context of intimate partner violence (IPV).</td>
</tr>
<tr>
<td><strong>Gendertrolling</strong></td>
<td>Malicious acts online involving the sending or submission of provocative emails or social-media posts, including rape and death threats. Similarly to trolling, also gendertrolling aspires to foment dispute and cultivate a following, inciting an angry or upsetting response from its intended target.</td>
</tr>
</tbody>
</table>

---

²⁸ This is a non-exhaustive list of terms related to forms of cyber violence that tend to target women and girls in the specific. Definitions in this section were not developed by EIGE.
³² (Ibid.)
Non-Consensual Pornography* A media-generated term used to describe the online distribution of private and sexually explicit images and videos without consent. Also labelled as Revenge Porn.

It is not recommended to use terms like non-consensual pornography or revenge porn. The term ‘pornography’ does not emphasise the non-consensual nature of the practices, and many perpetrators are not motivated by ‘revenge’ or by any personal feelings towards the victim.

Non-consensual intimate image (NCII) abuse is the term to be preferred35.

Revenge Porn* See Non-Consensual Pornography.

Sextortion36 The act of threatening to publish sexual content (images, videos, deepfakes, sexual rumours) to menace, coerce or blackmail someone, either for more sexual content or for money, sometimes both.

The perpetrator can be an ex-partner who obtains images or videos during a prior relationship, and aims to publicly shame and humiliate the victim, often in retaliation for ending a relationship.

Sexual Solicitation37 Receiving unwanted requests to talk about sex or do something sexual in a variety of online contexts, like sending sexually explicit images or engaging in technology-mediated sexual interactions.

It can lead to receiving abusive misogynist comments, harassment, and threats, particularly if the victim has rejected the requests in some way.

Slut-Shaming38 Stigmatising women and girls on the basis of their appearance, sexual availability, and actual or perceived sexual behavior. While slut-shaming targets victims of all ages, adolescent girls seem to be particularly affected by it.

This is a long-standing form of gender-based violence that is amplified in the cybersphere: it perpetuates the regulation of women and girls’ sexuality and curtails their freedom of speech online.

Upskirting39 Surreptitious and non-consensual filming of an unsuspecting woman’s thighs or private parts in public or private places. The material is usually published, traded, and exchanged on the internet without the victim’s knowledge.

Upskirting is a form of non-consensual intimate image (NCII) abuse.

Virtual Rape40 A situation when a person’s avatar (or digital representation of themselves) is subjected to simulated sexual violence by other avatars, most recently in three-dimensional virtual worlds like the Metaverse.

Note: * denotes a controversial term.

---

This brief is based on EIGE’s research on Cyberviolence against Women and Girls (CVAWG) carried out in 2021.

The report presents an analysis of existing legal and statistical definitions of the different forms of CVAWG across all EU Member States. Based on these findings, it proposes improvements to existing definitions used for statistical purposes and recommends their use across all EU Member States.

By means of this study, EIGE aims to contribute to better informed and evidence-based policies and measures against CVAWG. EIGE aims to support EU institutions and all EU Member States in collecting more evidence on CVAWG, contributing to reaching the goal of having a regular collection of CVAWG data across all EU Member States.

Clear and comprehensive definitions of CVAWG will enable the collection of reliable, disaggregated, and comparable data on the phenomenon at national level. This will result in improved policymaking and overall responses by the relevant authorities, such as law enforcement agencies and victim support services.

The full report is available at https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girls

You can explore all of EIGE’s previous reports and publications on CVAWG at https://eige.europa.eu/gender-based-violence/cyber-violence-against-women