

# Cyber Violence against Women and Girls

## Key Terms and Concepts

### 1. What is cyber violence against women and girls?

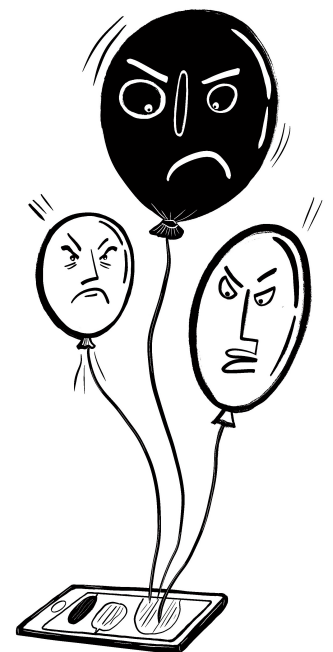
Digital platforms have often been celebrated for allowing equal opportunities for public self-expression, regardless of one's identity and status. Yet, **not everyone is welcome in the cyberspace**. The digital arena has become a breeding ground for a range of exclusionary and violent discourses and 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, surveil 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<sup>1</sup>.



<sup>1</sup> Sugiura, L. (2021). *The incel rebellion: The rise of the manosphere and the virtual war against women*. Emerald Group Publishing, Bingley. (<https://www.emerald.com/insight/publication/doi/10.1108/9781839822544>).

## 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<sup>2</sup>.

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<sup>3</sup>. 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<sup>4</sup>.

## 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<sup>5</sup>.

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<sup>6</sup>. 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**.

<sup>2</sup> Van der Wilk, A. (2018), *Cyber Violence and Hate Speech Online against Women*, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Brussels ([https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL\\_STU\(2018\)604979\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf)).

<sup>3</sup> Lomba, N., Navarra, C., and Fernandes, M. (2021), *Combating Gender-based Violence: Cyber violence – European added value assessment*, European Parliamentary Research Service, Brussels ([https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS\\_STU\(2021\)662621\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf)).

<sup>4</sup> EIGE (European Institute for Gender Equality) (2020), *Gender Equality Index Report*, Vilnius (<https://eige.europa.eu/publications/gender-equality-index-2020-report>).

<sup>5</sup> GREVIO (Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence) (2021), *General Recommendation N°1 on the digital dimension of violence against women*, Council of Europe, Strasbourg, 20 October 2021 (<https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>).

<sup>6</sup> EIGE (2018), *Gender equality and digitalization in the European Union*, Vilnius (<https://eige.europa.eu/publications/gender-equality-and-digitalisation-european-union>).

## 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<sup>7</sup>.



Among **migrants, second generations and ethnic or religious minorities**, cyber violence can lead to lower trust in institutions and ultimately damage social integration<sup>8</sup>.

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<sup>9</sup>.

## 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.

<sup>7</sup> FRA (European Union Agency for Fundamental Rights) (2014), *Violence against Women: An EU-wide survey – Main results*, Publications Office of the European Union, Luxembourg (<https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>).

<sup>8</sup> 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](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-challenges-to-women-human-rights_en.pdf)).

<sup>9</sup> Lomba, N., Navarra, C., and Fernandes, M. (2021), *Combating Gender-based Violence: Cyber violence – European added value assessment*, European Parliamentary Research Service, Brussels ([https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS\\_STU\(2021\)662621\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf)).

## 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<sup>10</sup>.
- Several studies highlight the links between stalking and cyber stalking<sup>11</sup>: a UK study found that over half (54 %) of cyber stalking cases involved a first encounter in the physical world<sup>12</sup>. Also, obtaining personal information through cyber stalking can lead to further violent actions both online and offline<sup>13</sup>.
- The negative impact of cyber stalking on the victims' well-being appears similar to that of stalking<sup>14</sup>. Cyber stalking victims report increased suicidal ideation, fear, anger, depression, and post-traumatic stress disorder symptomology<sup>15</sup>.

<sup>10</sup> FRA (2014), *Violence against Women: An EU-wide survey – Main results*, Publications Office of the European Union, Luxembourg (<https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>).

<sup>11</sup> Reynolds, B. W., and Fisher, B. S. (2018), 'The relationship between offline and online stalking victimisation: a gender-specific analysis', *Violence and Victims*, Vol. 33, No 4 (<http://dx.doi.org/10.1891/0886-6708.VV-D-17-00121>).

<sup>12</sup> Maple, C., Short, E., and Brown, A. (2011), *Cyber Stalking in the United Kingdom: An analysis of the ECHO pilot survey*, University of Bedfordshire, U.K. (<https://uobrep.openrepository.com/handle/10547/270578>).

<sup>13</sup> Gender and Policy Insights (2019), *When Technology Meets Misogyny: Multi-level, intersectional solutions to digital gender-based violence* (<https://gen-pol.org/wp-content/uploads/2019/11/When-Technology-Meets-Misogyny-GenPol-Policy-Paper-2.pdf>).

<sup>14</sup> DreBing, H., Bailer, J., Anders, A., Wagner, H., and Gallas, C. (2014), 'Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims', *Cyberpsychology, Behavior, and Social Networking*, Vol. 17, No 2, pp. 61–67 (<https://doi.org/10.1089/cyber.2012.0231>).

<sup>15</sup> Short, E., Linford, S., Wheatcroft, J. M., and Maple, C. (2014), 'The impact of cyberstalking: the lived experience – a thematic analysis', *Studies in Health Technology and Informatics*, Vol. 199, pp. 133–137 (<http://dx.doi.org/10.3233/978-1-61499-401-5-133>).

## 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<sup>16</sup>.
- 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<sup>17</sup>.
- 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<sup>18</sup>.

## 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 bullying have been bullied both online and offline, often by the same perpetrator(s)<sup>19</sup>.
- Across the OECD countries with available data, about 12 % of girls aged 15 report having been cyber bullied, compared with 8 % of boys<sup>20</sup>. 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<sup>21</sup>.
- Certain minority groups are more exposed to cyber bullying, such as LGBTIQ+ individuals and students with special needs<sup>22</sup>. Also, there are clear links between cyber bullying and mental health problems<sup>23</sup>.



<sup>16</sup> FRA (2019), *A Long Way to Go for LGBTIQ Equality*, Publications Office of the European Union, Luxembourg ([https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2020-lgbti-equality-1\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-lgbti-equality-1_en.pdf)).

<sup>17</sup> FRA (2014), *Violence against Women: An EU-wide survey – Main results*, Publications Office of the European Union, Luxembourg (<https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>).

<sup>18</sup> Amnesty International (2017), *Amnesty reveals alarming impact of online abuse against women*, press release (<https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/>).

<sup>19</sup> UNESCO (United Nations Educational, Scientific and Cultural Organization) (2019), *Behind the Numbers: Ending school violence and bullying*, Paris. (<https://unesdoc.unesco.org/ark:/48223/pf0000366483>).

<sup>20</sup> 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>).

<sup>21</sup> Cyberbullying Research Centre (2021), '2021 cyberbullying data' (<https://cyberbullying.org/2021-cyberbullying-data>).

<sup>22</sup> LearnSafe (2018), 'Who is most at-risk for cyberbullying?' (<https://learnsafe.com/who-is-most-at-risk-for-cyberbullying>).

<sup>23</sup> Nixon C. L. (2014), 'Current perspectives: the impact of cyberbullying on adolescent health', *Adolescent health, medicine and therapeutics*, 5, 143–158. (<https://doi.org/10.2147/AHMT.S36456>).

## 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.



- 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<sup>24</sup>.
- 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<sup>25</sup>.

## 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.

- The spread of such images can destroy victims' educational and employment opportunities as well as their intimate relationships. Victims are often threatened with sexual assault, stalked, harassed, fired from jobs, and forced to change schools. Some have committed suicide<sup>26</sup>.
- NCII abuse is closely linked to intimate partner violence (IPV). The perpetrator can be an ex-partner who aims to publicly shame and humiliate the victim, often in retaliation for ending the relationship. For this reason, media-generated terms like *non-consensual pornography* or *revenge porn* are often used. However, these terms are legally incorrect and create false impressions around the circumstances of the offense.
- Technological advances are enabling more and more realistic manipulation of images. This can be done using software such as Photoshop or AI tools to create synthetic media like deepfakes<sup>27</sup>.

<sup>24</sup> Amnesty International (2018), *Toxic Twitter*, Amnesty International, London (<https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2>).

<sup>25</sup> Gender and Policy Insights (2019), *When Technology Meets Misogyny: Multi-level, intersectional solutions to digital gender-based violence* (<https://gen-pol.org/wp-content/uploads/2019/11/When-Technology-Meets-Misogyny-GenPol-Policy-Paper-2.pdf>).

<sup>26</sup> Franks, M.A. (2019), 'The Crime of "Revenge Porn"', in: Alexander, L., and Ferzan, K. (eds), *The Palgrave Handbook of Applied Ethics and the Criminal Law*, Palgrave Macmillan, Cham. ([https://doi.org/10.1007/978-3-030-22811-8\\_28](https://doi.org/10.1007/978-3-030-22811-8_28)).

<sup>27</sup> Hao, K. (2021), 'Deepfake porn is ruining women's lives. Now the law may finally ban it', *MIT Technology Review* (<https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/>).

### 3. Glossary of terminology related to CVAWG<sup>28</sup>

**Cyber Flashing<sup>29</sup>** 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.

**Deepfake<sup>30</sup>** 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.

**Digital Voyeurism<sup>31</sup>** 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*.

**Downblousing<sup>32</sup>** 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.

**Doxing<sup>33</sup> (also spelled Doxing)** 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).

**Gendertrolling<sup>34</sup>** 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.

<sup>28</sup> 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.

<sup>29</sup> GREVIO (2021), *General Recommendation N°1 on the digital dimension of violence against women*, Council of Europe, Strasbourg, 20 October 2021 (<https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>).

<sup>30</sup> van Huijstee, M., van Boheemen, P., and Das D., 2021, *Tackling deepfakes in European policy* European Parliamentary Research Service, Brussels. ([https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_STU\(2021\)690039](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039)).

<sup>31</sup> Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A., and Scott, A. J. (2020), *Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery*, Routledge, London.

<sup>32</sup> (Ibid.)

<sup>33</sup> European Women's Lobby (2017), *#HerNetHerRights Resource Pack on ending online violence against women & girls in Europe* ([https://www.womenlobby.org/IMG/pdf/hernetherights\\_resource\\_pack\\_2017\\_web\\_version.pdf](https://www.womenlobby.org/IMG/pdf/hernetherights_resource_pack_2017_web_version.pdf)).

<sup>34</sup> Lumsden, K., and Morgan, H. M. (2018), 'Cyber-trolling as symbolic violence: deconstructing gendered abuse online', in N. Lombard (ed.) *The Routledge handbook of Gender and Violence*, Chapter 9, Routledge, London.

**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 preferred<sup>35</sup>.

**Revenge Porn\*** See *Non-Consensual Pornography*.

**Sextortion**<sup>36</sup> 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 Solicitation**<sup>37</sup> 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-Shaming**<sup>38</sup> 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.

**Upskirting**<sup>39</sup> 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 Rape**<sup>40</sup> 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.

<sup>35</sup> Council of Europe Cybercrime Convention Committee (2018), *Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018*, Strasbourg (<https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914>).

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

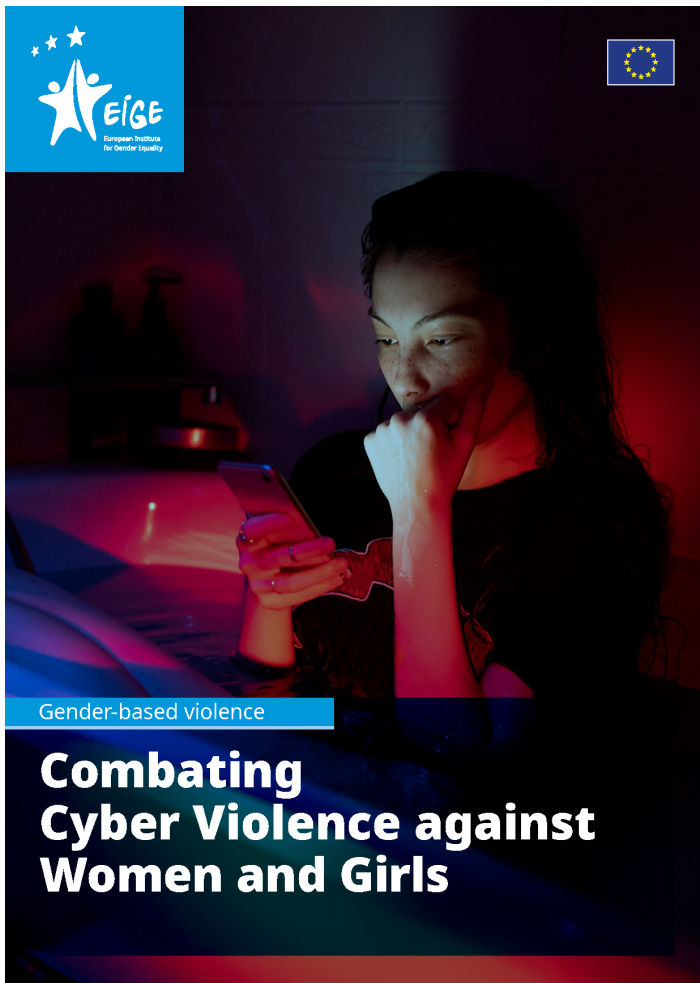
<sup>37</sup> Henry, N. and Powell, A. (2016), *Sexual violence in the digital age*, Routledge, London.

<sup>38</sup> Goblet, M., and Glowacz, F. (2021), 'Slut Shaming in Adolescence: A Violence against Girls and Its Impact on Their Health', *International Journal of Environmental Research and Public Health*, 18(12), 6657. (<http://dx.doi.org/10.3390/ijerph18126657>).

<sup>39</sup> Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A., and Scott, A. J. (2020), *Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery*, Routledge, London.

<sup>40</sup> Henry, N., and Powell, A. (2018), 'Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research', *Trauma, Violence, & Abuse*, 19(2). (<https://doi.org/10.1177/1524838016650189>).





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>

## European Institute for Gender Equality

The European Institute for Gender Equality (EIGE) is the EU knowledge centre on gender equality. EIGE supports policymakers and all relevant institutions in their efforts to make equality between women and men a reality for all Europeans by providing them with specific expertise and comparable and reliable data on gender equality in Europe.

© European Institute for Gender Equality, 2022

Graphic illustrations: © Eglė Narbutaitė

Reproduction is authorised provided the source is acknowledged.



European Institute for Gender Equality  
Gedimino pr. 16  
LT-01103 Vilnius  
Lithuania

## Contact details

[eige.europa.eu](https://eige.europa.eu)   
[facebook.com/eige.europa.eu](https://facebook.com/eige.europa.eu)   
[twitter.com/eige\\_eu](https://twitter.com/eige_eu)   
[youtube.com/user/eurogender](https://youtube.com/user/eurogender)   
[linkedin.com/company/eige](https://linkedin.com/company/eige)   
[eige.sec@eige.europa.eu](mailto:eige.sec@eige.europa.eu)   
+370 52157444 