

Co-funded by the Erasmus+ Programme of the European Union

Cyber violence against women



This finding is corroborated by a 2014 survey by the Pew Research Center in the United States , which found that though men are slightly more likely than women to experience relatively 'mild' forms of online harassment (such as name-calling and embarrassment), women (particularly young women aged 18-24) disproportionately experience severe types of cyber harassment, namely cyber stalking and online sexual harassment.





The results of these studies are echoed by further research, exposing the limitations in taking a gender blind approach to cyber violence; the current evidence suggests that the forms of violence and the resulting harm is experienced differently by women and men.

In addition, experts have warned against conceptualising cyber VAWG as a completely separate phenomenon to "real world" violence, when in fact it is more appropriately seen as a continuum of offline violence. For example, cyber stalking by a partner or ex-partner follows the same patterns as offline stalking and is therefore intimate partner violence, simply facilitated by technology. **Evidence confirms this** continuum: a UK study of cyber stalking found that over half (54 %) of the cases involved a first encounter in a real-world situation.



There are various forms of cyber VAWG, including, but not limited to, cyber stalking, non-consensual pornography (or "revenge porn"), gender-based slurs and harassment, "slutshaming", unsolicited pornography, "sextortion", rape and death threats, "doxing", and electronically enabled trafficking.



Cyber Stalking



Stalking is stalking by means of email, text (or online) messages or the internet. Stalking involves repeated incidents, which may or may not individually be innocuous acts, but combined undermine the victim's sense of safety and cause distress, fear or alarm. Acts can include:

- Sending emails, text messages
 (SMS) or instant messages that are
 offensive or threatening;
- Posting offensive comments about the respondent on the internet;
- Sharing intimate photos or videos of the respondent, on the internet or by mobile phone.
- To be considered as cyber stalking, these acts must take place repeatedly and be perpetrated by the same person.

Cyber Harassment



Cyber harassment can take many forms, but for the purposes of this paper, it can include:

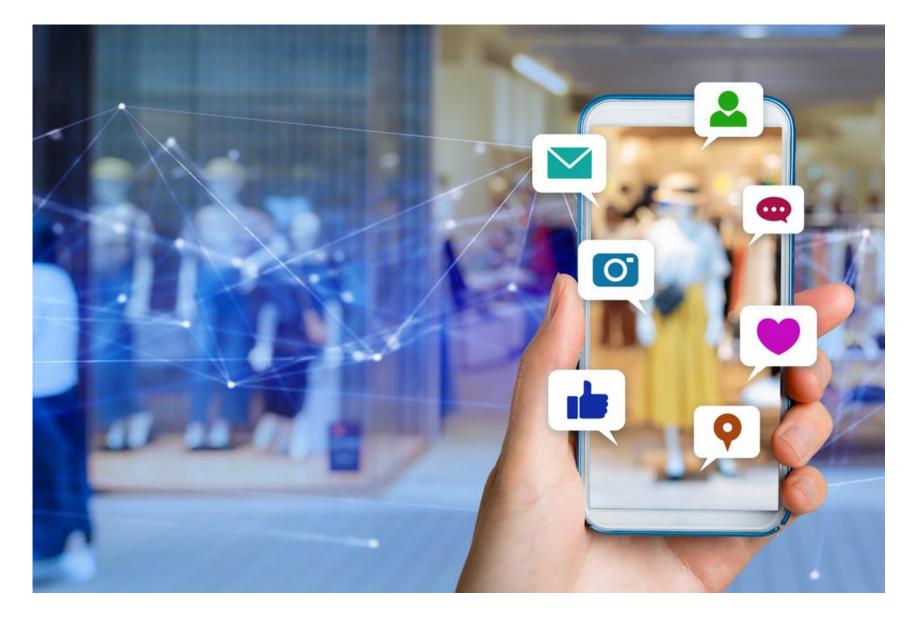
- Unwanted sexually explicit emails, text (or online) messages
- Inappropriate or offensive advances on social networking websites or internet chat rooms;
- Threats of physical and/or sexual violence by email, text (or online) messages;
- Hate speech, meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and other traits (such as sexual orientation or disability).



Non-consensual Pornography Also known as cyber exploitation or "revenge porn", non-consensual pornography involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images. The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship, and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship. However, perpetrators are not necessarily partners or ex-partners and the motive is not always revenge. Images can also be obtained by hacking into the victim's computer, social media accounts or phone, and can aim to inflict real damage on the target's 'real-world' life (such as getting them fired from their job).



There have been multiple publicised cases of female victims of non-consensual pornography in EU Member States and the US over recent years, several of whom committed suicide as a result. Research suggests that up to 90 % of revenge porn victims are female and that the number of cases is increasing. There are also a growing number of websites dedicated to sharing revenge porn, where users can submit images alongside personal information such as the victim's address, employer and links to online profiles



An additional related trend with equally devastating impacts on victims is the live-broadcasting of incidents of sexual assault and rape via social media. So far in 2017 there have already been two high-profile cases: one in Sweden and the other in the U.S., of victims whose rape was streamed online using the 'Facebook live' function.

The following recommendations are in line with the international human rights legal framework, including the Istanbul Convention, and are based on a review of existing literature and evidence. They ultimately aim to support EU Member States to improve institutional responses to cyber VAWG, in order to protect women both online and offline.

- 1. Policy responses should be formulated in recognition of the fact that cyber VAWG is a form of VAW. Strategies for addressing cyber VAWG must also include the voices of women who are victims of the phenomenon.
- 2. In the immediate future, definitions of cybercrime on the Migration and Home Affairs website should be updated to include forms of cyber VAWG, or at the minimum, should include misogyny in the third part of its definition
- 3. The EU should aim towards agreeing on definitions of forms of cyber VAWG and incorporate these forms of violence into EU legislation, to ensure that victims of cyber VAWG in Member States have access to justice and specialised support services.
- 4. A priority should be to improve gender-disaggregated data at EU level on the prevalence and harms of cyber VAWG, and to develop indicators to measure the effectiveness of interventions.
- 5. Any approach to tackling the phenomenon must not deny women and girls their place in the larger public space they gain from internet connection. The upcoming EU-wide Survey on GBV should include a question about whether women have avoided online spaces for fear of experiencing cyber VAWG.

- 6. There is a need for quantitative and qualitative research that examines system responses, based on a victims' perspective.
- 7. Training on cyber VAWG with a gender perspective should be introduced to police responses to cybercrime
- 8. There is a need for awareness-raising campaigns educating women and girls about cyber VAWG, their legal rights and available support services
- 9. Prevention measures should be developed that include the ICT sector, including adoption of selfregulatory standards to avoid harmful gender stereotyping and the spreading of degrading images of women, or imagery that associates sex with violence.
- 10. It is important for EU level institutions and agencies combatting cybercrime to tackle gendered forms of cybercrime; particularly the online luring or "recruitment" of women and girls into harmful situations such as trafficking.



STOP VIOLENCE Against Women



