European Institute
for Gender Equality

Cyber violence against women and girls

CONTENTS

Introduction 1

Cyber violence as a form of gender-based violence 1

What is Cyber violence against women and girls? 1

Defining forms of cyber violence against women and girls 2

Data availability and research 3

Law enforcement responses 4

Conclusions and recommendations 5

Endnotes 6

Introduction

The increasing reach of the internet, the rapid spread of mobile information, and the widespread use of social media, coupled with the existing pandemic of violence against women and girls (VAWG) ([1]), has led to the emergence of cyber VAWG as a growing global problem with potentially significant economic and societal consequences ([2]).

Research shows ([3]) that one in three women will have experienced a form of violence in her lifetime, and despite the relatively new and growing phenomenon of internet connectivity, it is estimated that one in ten women have already experienced a form of cyber violence since the age of 15 ([4]). Access to the internet is fast becoming a necessity for economic well-being ([5]), and is increasingly viewed as a fundamental human right ([6]); therefore it is crucial to ensure that this digital public space is a safe and empowering place for everyone, including women and girls.

In order to better understand the nature and prevalence of cyber VAWG, the European Institute for Gender Equality (EIGE) has recently conducted desk research that aimed to identify and analyse the existing research on different forms of cyber VAWG and assess the availability of survey and administrative data on the phenomenon. The findings of this research and the resulting recommendations form the basis of this paper.

Cyber violence as a form of gender-based violence

What is cyber violence against women and girls?

To date, cyber VAWG has not been fully conceptualised or legislated against at EU level. Furthermore, there has been no gender-disaggregated EU-wide survey on the prevalence and harms of cyber VAWG and there is limited national-level research within EU Member States. However, the research that is available suggests that women are disproportionately the targets of certain forms of cyber violence compared to men. For example, in a survey of more than 9,000 German Internet users aged 10 to 50 years, women were significantly more likely than men to have been victims of online sexual harassment and cyber stalking, and the impacts of these forms of violence were more traumatic for victims ([7]).

This finding is corroborated by a 2014 survey by the Pew Research Center in the United States ([8]), 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 ([9]).

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 ([10]), simply facilitated by technology ([11]). 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 ([12]).

Furthermore, data from the 2014 FRA survey shows that 77 % of women who have experienced cyber harassment [13] have also experienced at least one form of sexual or/and physical violence from an intimate partner; and 7 in 10 women (70 %) who have experienced cyber stalking [14], have also experienced at least one form of physical or/and sexual violence from an intimate partner [15].

Defining forms of cyber violence against women and girls

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, 'slut-shaming', unsolicited pornography, 'sextortion', rape and death threats, 'doxing', and electronically enabled trafficking [16].

In this paper, EIGE's primary focus will be on those forms of cyber VAWG that most closely link to intimate partner violence (IPV), due to our existing knowledge of the severe impact of IPV on victims; these include: cyber stalking, cyber harassment and non-consensual pornography.

As with IPV experienced offline, cyber VAW can manifest as various forms of violence, including sexual, psychological and, as growing trends would indicate, economic, whereby the victim's current or future employment status is compromised by information released online. The potential for violence in the cyber-sphere to manifest psychically should also not be discounted. However further research into the experiences of victims of cyber VAWG is needed to better understand its impact.

There are no agreed definitions of these forms of cyber VAWG at EU level; therefore the following explanations are based on a review of the literature.

Cyber Stalking

Cyber 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 [17]. Research suggests that up to 90 % of revenge porn victims are female [18] and that the number of cases is increasing [19]. 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 [20].

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 [21].

Data availability and research

Data on cyber VAWG in the EU is scarce and consequently very little is known about the actual percentage of victims of cyber VAWG and the prevalence of harm. The best information available at EU level comes from the European Agency for Fundamental Rights' (FRA) European Survey on Violence Against Women (VAW) (2014), which included questions on cyber stalking [22] and cyber harassment [23]. However, as this survey was the first to collect data on these forms of cyber VAWG across the EU, there is no means by which to trace the evolution of the phenomena and trends in victim numbers over time.

Apart from one (2008 Danish) survey, it was not possible to identify any nationally representative surveys at Member State level on the prevalence of cyber VAWG [24].

Given that in most Member States forms of cyber VAWG are not criminalised, police or justice data on the phenomenon is scarce. In Member States where forms of cyber VAWG are criminalised, the data collected is lacking disaggregation by sex of the victim and perpetrator, and the relationship between them, which limits the usefulness of the data [25]. This lack of data hampers the ability to conduct a gendered analysis of cyber violence and a comparison of online and offline VAWG.

In addition to addressing the aforementioned gaps, more research is needed in the following areas:

1. Use of online adverts or postings to lure women into potentially harmful situations ('recruitment').

2. Assessment of the severity of harm experienced by victims of forms of cyber VAWG, and the impact on their lives.

3. Good practices in police and justice responses to cyber VAWG, including from a victim's perspective.

4. Identification and analysis of risk factors and risk assessment procedures, to prevent harm and re-victimisation.

Law enforcement responses

Several Member States have recently adopted legislation targeting forms of cyber VAWG; for example, provisions criminalising revenge porn have been enacted in the U.K., France, Germany and Malta, with policies currently pending in Ireland and Slovenia. While this is a step in the right direction, studies suggest that current legal and policy approaches in the EU fail to adequately capture the social and psychological harm resulting from the use of sexual imagery to harass, coerce or blackmail women (26).

Furthermore, research reveals that the response of the criminal justice sector to women victims of cyber VAWG is inadequate. For example, of the 1 160 incidents of revenge porn reported during the first six months after its criminalisation in the U.K., 61 % resulted in no further action pursued against the alleged perpetrator (27).

In 2013 the End Violence against Women Coalition (EVAW) gathered accounts at a roundtable on enforcement and prosecution of 'violence and harassment' online, reporting concerns that criminal justice authorities took a different, and less effective, approach to violence and harassment perpetrated online compared to offline. Several participants themselves had experienced 'wholly inadequate police responses' when reporting a crime perpetrated online (28).

Studies echo these concerns, revealing women's frustration with police who tend to treat each individual online communication as a discrete act, rather than considering the cumulative impact of abuse (29). This reflects broader concerns about the criminal justice system's response to VAWG in general (and particularly IPV). Moreover, victim blaming attitudes persist, especially in cases of revenge porn, demonstrating a lack of understanding and awareness. This is compounded by the fact that (according to a 2014 survey in the U.S.) more than half of stalking and cyber stalking victims did not acknowledge their own experience as a crime (30).

This inadequate criminal justice response can be attributed in part to the false dichotomy between online and offline VAWG, which results in police discounting and minimising the harms of cyber VAWG, and constructing victims' experiences as "incidents" rather than patterns of behaviour over time.

These findings reveal the need to design effective policy interventions at both the EU and Member State level, including but not limited to: training for police and justice sector staff on cyber VAWG and awareness-raising campaigns.

Good practices

Legislation

In the UK, in April 2015 it became a criminal offence with maximum two-years imprisonment to share private sexual photographs or videos without the subject's consent providing the intent of causing distress to those targeted (31). In September 2016 it was announced that more than 200 people had been prosecuted since the law came into effect (32).

Meanwhile in 2016, France adopted the 'Digital Republic Law,' which entails a harsher sanctioning of those found guilty of revenge porn. Under new legislation perpetrators face a two year prison sentence or € 60 000 fine (33).

Similar provisions were enacted by a German court, which in 2014 made it illegal to store intimate photographs of a former partner after they have called for their deletion (34).

Research and interventions

In 2009, the U.K. launched The National Centre for Cyberstalking Research (NCCR) (35), which aims to provide research and analysis into the prevalence, motivations, impacts and risk assessment of cyber VAWG. In 2011 the centre published the results of a study on the prevalence, nature and impact of cyber stalking (36) and is currently conducting a survey investigating the impact and prevalence of revenge porn. Subsequently in 2015, a helpline for victims of revenge porn was established, receiving almost 2 000 calls in its first six months (37).

From July 2017, Slovenia will launch the project 'CYBERVAW', which aims to develop awareness-raising and education activities that spread a clear message of zero tolerance to VAWG, with a specific focus on prevention of gender-based cyber violence and harassment as a form of VAWG (38).

Conclusions and recommendations

In sum, due to the current lack of research and data at EU level, we cannot adequately quantify the prevalence or impact of cyber VAWG in the EU. However, the mounting evidence suggests that it is a growing phenomenon disproportionately affecting women and girls, with severe impacts on victims' 'real' lives. In order to better determine the prevalence and risk factors of, and effective policy responses to, cyber VAWG, a priority should be the development of measurement and quantification tools of these types of acts.

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 ([39]).

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 self-regulatory 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.

Endnotes

[1] "Violence against women" is defined by the Council of Europe as 'a violation of human rights and a form of discrimination against women and shall mean all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life'. (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008482e)

[2] UN Broadband Commission for Digital Development (2015). *Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call.* Available at: http://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?vs=4259

[3] World Health Organization, Department of Reproductive Health and Research, London School of Hygiene and Tropical Medicine, South African Medical Research Council (2013). *Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence*, p. 2. Available at: http://www.who.int/reproductivehealth/publications/violence/9789241564625/en/.

[4] European Union Agency for Fundamental Rights (2014). *Violence against women: an EU-wide survey – Main results.* Luxembourg: Publications Office of the European Union, p. 104. Available at: http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

[5] Goal 9.C of the Sustainable Development Goals aims to provide universal and affordable access to the Internet, in recognition of its developmental potential (See: https://sustainabledevelopment.un.org/sdg9 and https://www.one.org/us/2015/09/26/the-connectivity-declaration-demanding-internet-access-for-all-and-implementation-of-the-global-goals/).

[6] UN Human Rights Council (2016). Non-binding resolution. Article 32: *The promotion, protection and enjoyment of human rights on the Internet.* Available at: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.

[7] Staude-Müller, F., Hansen, B., Voss, M. (2012) How stressful is online victimization? Effects of victim's personality and properties of the incident. *European Journal of Developmental Psychology, 9*(2). Available at: http://www.tandfonline.com/doi/abs/10.1080/17405629.2011.643170.

[8] Pew Research Center (2014). *Online Harassment.* Available at: http://www.pewinternet.org/2014/10/22/online-harassment/.

[9] Maple, C., Shart, E., Brown, A. (2011). *Cyber stalking in the United Kingdom: An Analysis of the ECHO Pilot Survey.* University of Bedfordshire. Available at: https://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf.

[10] "Intimate Partner Violence" is defined as: A pattern of assaultive and coercive behaviours, including physical, sexual and psychological acts, as well as economic coercion, which adults or adolescents may use against their intimate partners without their consent. The resulting feelings of shame, fear and helplessness lead to low levels of reporting and, subsequently, relatively few convictions. The largest burden of intimate partner violence is inflicted by men against their women partners (http://eige.europa.eu/rdc/thesaurus/terms/1265).

[11] Burney, E. (2009). *Making People Behave: Anti-Social Behaviour. Politics and Policy.* Routledge.
And: Chakraborti, N. and Garland, J. (2009). *Hate Crime: Impact, Causes and Responses.* 2nd Ed. London: Sage Publications Ltd.

[12] According to a large number of investigations, among which Pathé and Mullen (1997) emphasise, women experience cyberstalking in a more traumatic way than men. (Pathé, M. and Mullen, P.E. (1997). The impact of stalkers on their victims. [Abstract]. *British Journal of Psychiatry Jan 1997, 170*(1) 12-17. Available at: https://www.ncbi.nlm.nih.gov/pubmed/9068768#).

[13] 11 % of women have received unwanted, offensive sexually explicit emails or SMS messages, or inappropriate, offensive advances on social networking sites (FRA (2014). *Violence against women: an EU-wide survey.* Main results report, 29, 95. Available at: http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report).

[14] 5 % of women in the EU have experienced one or more forms of cyber stalking since the age of 15 (FRA, 2014: 87). Cyber stalking in this case included stalking by means of email, text messages or over the internet.

[15] Statistical analysis made by EIGE. 1044 women have suffered one or more of the three forms of cyber stalking and out of those women, 727 have experienced at least one or more forms of physical or/and sexual violence from an intimate partner. As part cyber harassment, out of 677 women who stated having suffered at least one of the three forms identified as cyber harassment, 518 (77 %) have also experienced at least one form of physical or/and sexual violence from an intimate partner.

[16] There are no agreed definitions at EU level. An explanation of each form of cyber VAWG can be found here: http://wmcspeechproject.com/online-abuse-101/.

[17] For example:

- Italian woman Tiziana Cantone committed suicide in 2016 following revenge porn, she had previously been fired from her job: http://www.bbc.com/news/world-europe-37377286;
- 15 year-old Amanda Todd from Canada committed suicide in 2012 after a man circulated images of her online without her consent: http://www.bbc.co.uk/newsbeat/article/19960162/amanda-todd-memorial-for-teenage-cyberbullying-victim;
- 17 year-old Julia Rebecca from Piaui, Brazil took her own life in 2013 after sexually graphic footage of herself and a partner were posted online without her consent: https://www.bustle.com/articles/9485-revenge-porn-legislation-called-for-in-brazil-following-17-year-olds-suicide.

[18] According to a survey in 2015 by the Cyber Civil Rights Initiative: https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf. (NB this survey used a convenience sample of 1,606 respondents).

[19] See: https://www.theguardian.com/technology/2015/jul/15/revenge-porn-cases-increase-police-figures-reveal.

[20] When one domain is shut down, it is not uncommon to find a number of duplicates. The most prolific example of online revenge porn, 'Is Anyone Up.com,' at one point received 350 000 hits daily and inspired a sequence of 'spin-off' sites by similar names after its removal from the web in 2012: https://www.theguardian.com/culture/us-news-blog/2012/dec/06/hunter-moore-isanyone-up-revenge-porn-website.

[21] http://www.bbc.com/news/world-europe-38717186 and http://www.independent.co.uk/news/world/americas/chicago-teenager-gang-rape-facebook-live-video-dozens-watched-a7642866.html.

[22] Cyberstalking: stalking by means of email, text messages or the internet – affects young women in particular. Four per cent of all 18 to 29-year-old women, or 1.5 million, in the EU-28 have experienced cyberstalking in the 12 months before the interview, compared with 0.3 % of women who are 60 years old or older. (FRA (2014). *Violence against women: an EU-wide survey.* Main results report. Available at: http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report).

[23] Sexual harassment: non-verbal forms including cyber harassment, 11 % of women have received unwanted, offensive sexually explicit emails or SMS messages, or offensive, inappropriate advances on social networking sites (referring to experiences since the age of 15). (FRA (2014). *Violence against women: an EU-wide survey.* Main results report. Available at: http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report).

[24] K. Helweg-Larsen, N. Schütt, and H.B. Larsen (2012). Predictors and protective factors for adolescent Internet victimization: results from a 2008 nationwide Danish youth survey. *Acta Paediatrica, 101*(5), 533-539.

[25] For example, England and Wales, which criminalised revenge porn in 2014. The BBC analysed freedom of information requests from 31 police forces in England and Wales between April and December 2015, though notably the sex of the victim and the relationship to the perpetrator is not recorded in the majority of cases, limiting the usefulness of the data: https://docs.google.com/spreadsheets/d/1T6bqWcss4JKu7L9LV11VLy-z8FeY-PUP42ZW-SNe3Gmw/edit?usp=sharing.

[26] Henry, N. and Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian and New Zealand Journal of Criminology, 48*(1), 105.

[27] http://www.bbc.com/news/uk-37278264.

[28] EVAW (2013). *New Technology: Same Old Problems. Report of a roundtable on social media and violence against women and girls*. Available at: http://www.endviolenceagainstwomen.org.uk/resources/61/new-technology-same-old-problems-dec-2013, p. 5.

[29] See endnote 11.

[30] Nobles, M.R., Reyns, B.W., Fox, K.A. and Fisher, B.S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly, 31*(6), 53-65.

[31] Crown Prosecution Service guidelines on prosecuting the offence of disclosing private sexual photographs and films. Available at: http://www.cps.gov.uk/legal/p_to_r/revenge_pornography/.

[32] Crown Prosecution Service (2016) *Violence against women and girls: Crime report 2015-16*, p. 11. Available at: http://www.cps.gov.uk/publications/docs/cps_vawg_report_2016.pdf.

[33] https://www.transatlantic-lawyer.com/2016/09/france-the-new-digital-law-is-adopted/.

[34] https://www.theguardian.com/technology/2014/may/22/revenge-porn-victims-boost-german-court-ruling.

[35] https://www.beds.ac.uk/research-ref/irac/nccr.

[36] Maple, C., Shart, E., Brown, A. (2011). *Cyber stalking in the United Kingdom: An Analysis of the ECHO Pilot Survey*. University of Bedfordshire. Available at: https://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf.

[37] UK Government Press Release (2015). Available at: https://www.gov.uk/government/news/hundreds-of-victims-of-revenge-porn-seek-support-from-helpline.

[38] Report of the Office of the High Commissioner for Human Rights on ways to bridge the gender digital divide from a human rights perspective – response of Slovenia. Available at: http://www.ohchr.org/Documents/Issues/Women/WRGS/GenderDigital/SLOVENIA.docx.

[39] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.

MH-04-17-543-EN-N

VISUALS: "Black White Social Media Icons" (c)Alfredo, CC BY 3.0 /transparency effect added to original

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.

ISBN 978-92-9493-896-1 doi:10.2839/876816