

# GBV AoR HELPDESK

## Learning Series on Technology-Facilitated Gender-Based Violence

### Learning Brief 1: Understanding technology-facilitated gender-based violence



#### Introduction

Digital and other information and communication technologies (ICTs) are potentially powerful tools for catalyzing women's empowerment and gender equality. Digital tools and platforms are enabling tremendous opportunities for women and girls' economic, social and political inclusion, participation and agency, providing women and girls with unprecedented access to information and services and facilitating feminist organizing and campaigning.<sup>1</sup> Technology is also however, changing women and girls' experiences of violence. Mobile phones and the Internet are being used to intimidate, harass, exploit, abuse, stalk, threaten and blackmail women and girls, with devastating consequences for individuals and potentially for women's rights more broadly.

Technology-facilitated gender-based violence (TFGBV)<sup>2</sup> is not a new problem; the Association for Progressive Communications (APC) has been documenting how ICTs are utilized to perpetrate GBV since 2005.<sup>3</sup> However, evidence suggests it is a growing one. As more women and girls around the world have access to mobile phones and the Internet, more are exposed to violence perpetrated using this technology by a wide range of people - current and former partners, acquaintances and strangers. COVID-19 has exacerbated the problem, not only accelerating the already rapid pace of global digital transformation and increasing reliance and use of digital technology, but also accelerating women and girls' exposure to technology-related harassment, abuse and violence due

---

<sup>1</sup> It is important to note there are significant barriers hindering women and girls' access to, and ability to use technology. See GBV AoR (2019) *Harnessing Technology to Prevent, Mitigate and Respond to GBV in Humanitarian Settings* for further discussion of the digital gender divide and of the different ways in which technology is being used in efforts to address GBV.

<sup>2</sup> 'Online', 'digital' and 'cyber' violence are all common terms used to describe violence women and girls experience via the internet. The broader terms 'technology-facilitated violence' and 'technology-related violence' are used by many actors, and in this learning series, to be inclusive of all the ways that technology is used to perpetrate violence against women and girls, including online violence as well as other violence perpetrated using ICTs, such as mobile phone calls, texts and cameras. The UN Special Rapporteur on Violence Against Women uses the term 'online and ICT-facilitated forms of violence against women' in recognition that online violence does not adequately capture the different ways technology is used to perpetrate violence against women and girls. Other researchers have also highlighted different ways technology is used to perpetrate GBV, including Bluetooth connections between devices and location-based technologies such as Global Positioning Systems used in harassment and/or stalking contexts. The terms 'digital' and 'online' violence are also used where relevant throughout these learning briefs to refer to specific forms of technology-facilitated GBV.

<sup>3</sup> Fascendini, F. and Fialová, K. (2011) *Voices from digital spaces: Technology related violence against women*, Association for Progressive Communications: <https://www.apc.org/en/pubs/voices-digital-spaces-technology-related-violence>

to the shift of many activities online in response to the pandemic.<sup>4</sup>

As a result, TFGBV is rapidly emerging as a significant form of gender-based violence (GBV) globally, including in contexts impacted by conflict, disaster and other humanitarian emergencies. Women and girls have the right to live free from violence online, as they do offline.<sup>5</sup> Duty bearers, including governments and humanitarian actors have obligations to fulfill women's human rights, including before, during and after crises. Yet little is known about TFGBV or about effective approaches to addressing it in emergency-affected and fragile settings. To prevent and respond to this emerging problem as part of wider GBV in emergencies (GBViE) efforts, it is critical that the GBViE community<sup>6</sup> understands TFGBV and develops effective strategies and capabilities to address it.

This learning series seeks to: 1) build basic knowledge about TFGBV; 2) highlight existing strategies for preventing and responding to TFGBV that may be adapted for use in emergency-affected and fragile contexts; and 3) suggest priority actions for different stakeholders to take to begin to address the problem. The series is informed by research and practice evidence,<sup>7</sup> including review of published and grey literature and interviews with 25 researchers, practitioners and activists working across diverse contexts globally.<sup>8</sup> Those interviewed included GBV specialists, women's and digital rights activists, researchers and other experts working at the intersection of technology and GBV.

This first learning brief in the series provides a definition and overview of TFGBV behaviors, looks at prevalence and how TFGBV is manifesting in emergency contexts, and the impacts it has on women and girls.<sup>9</sup> It also suggests five priority actions GBV practitioners and specialists can take to help build knowledge, awareness and evidence about TFGBV.

## What is technology-facilitated violence against women and girls and how does it relate to offline violence?

*All forms of online gender-based violence are used to control and attack women and to maintain and reinforce patriarchal norms, roles and structures and an unequal power relationship. This is particularly evident when violence, threats and harassment follow speeches or expression related to gender equality and feminism, or where defenders of women's rights are targeted for their work.<sup>10</sup>*

<sup>4</sup> UN Women (2020) *COVID-19 and violence against women and girls: Addressing the shadow pandemic*, UN Women: <https://www.unwomen.org/en/digital-library/publications/2020/06/policy-brief-covid-19-and-violence-against-women-and-girls-addressing-the-shadow-pandemic>; Dunn, S. (2020) *Technology-Facilitated Gender-Based Violence: An Overview*, The Centre for International Governance Innovation: <https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview>

<sup>5</sup> See Learning Brief 3 for further discussion of the international human rights framework relevant to TFGBV.

<sup>6</sup> The GBViE community includes GBV practitioners, researchers, specialists and policy-influencers and makers at country, regional and global levels.

<sup>7</sup> In addition to undertaking review of literature and resources, the Helpdesk partnered with the GBV AoR Community of Practice (CoP) to undertake a survey on TFGBV among members to seek input on how TFGBV is manifesting in different contexts, how services are responding and challenges in addressing the problem. CoP members were invited to participate in an interview to share their knowledge, experience and expertise in addressing TFGBV.

<sup>8</sup> Those interviewed included GBV specialists and service providers working with survivors of TFGBV, researchers, women's rights activists, policy advisors and program managers, the majority in middle and low income contexts. Informants work for community-based and national NGOs, international NGOs, research institutions, UN agencies in Africa, Asia-Pacific, the Middle East, Europe and North America. While they are not individually named to protect the identity and location of some informants, they are all acknowledged and thanked for sharing their time, experience, knowledge and expertise in this area.

<sup>9</sup> The second learning brief focuses on strategies and actions for GBViE practitioners and specialists to prevent and respond to TFGBV in emergency-affected and fragile contexts, and the third looks at wider implications of TFGBV on women's rights and gender equality and provides recommendations on priority actions that humanitarian agencies, donors and online industries can take to begin to fulfil their responsibilities to prevent and respond to TFGBV in emergency-affected settings.

<sup>10</sup> A/HRC/38/47, *Report of the Special Rapporteur on violence against women, its causes and consequences on online*

TFGBV, also called online violence, cyberviolence and digital violence, is “any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of information, communication technologies (ICT), such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.”<sup>11</sup> The broader term TFGBV is used to be inclusive of violence perpetrated by technology not reflected in the terms ‘online’, ‘cyber’ or ‘digital’. For example, violence perpetrated by mobile phone calls and texts, Global Positioning Systems (GPS) and Bluetooth.

GBV perpetrated using digital tools and platforms is not a separate phenomenon to offline violence; it is part of the continuum “of multiple, recurring and interrelated forms of gender-based violence against women and girls” that occur throughout women’s lives.<sup>12</sup> TFGBV is rooted in, driven by, replicates and reinforces the same structural gender inequalities and sexist and misogynistic beliefs, norms and institutions that underpin other forms of GBV.<sup>13</sup> It is also rooted in racism, homophobia, transphobia and other forms of discrimination.<sup>14</sup> Violence and abuse online are simply an extension of these acts offline.<sup>15</sup>

## What are common technology-facilitated gender-based violence behaviors?

TFGBV includes a wide range of behaviors and acts<sup>16</sup> perpetrated by intimate partners, acquaintances, strangers and institutions. The motivations behind perpetration of acts of TFGBV differ, but commonly include seeking to humiliate, intimidate or cause fear, retribution, embarrass, coerce, control and/or exploit.<sup>17</sup> Online violence is also used to silence and undermine women’s and girl’s voices and rights, and their participation in public forums, debates and discussions. Common behaviors used by perpetrators are described below. Further information about different types and terms can be found in Annex 1.<sup>18</sup>

**Threats:** Threats include violent, aggressive or threatening speech or content that expresses an intention to harm a woman or girl or her family or friends. They may also be made against groups of women expressing political or other views or opinions.<sup>19</sup> Threats may be made via mobile phone calls or text, emails, social media and other online communication applications and platforms and websites. Threats against women and girls made via technology are commonly of a sexual nature, though may also relate to physically attacking, hurting or killing an individual or group of women.

---

*violence against women and girls from a human rights perspective:*

<https://digitallibrary.un.org/record/1641160?ln=en#record-files-collapse-header>

<sup>11</sup> Ibid

<sup>12</sup> Association for Progressive Communications (APC) (2017) *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences*: [https://www.apc.org/sites/default/files/APCSubmission\\_UNSR\\_VAW\\_GBV\\_0\\_0.pdf](https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf)

<sup>13</sup> APC (2017)

<sup>14</sup> Dunn (2020)

<sup>15</sup> Dunn (2020)

<sup>16</sup> Hinson, L., Mueller, J. O’Brien-Milne, L. and Wandera, N. (2018) *Technology-Facilitated Gender-Based Violence: What is it, and how do we measure it?*, International Research Centre on Women, Washington:

<https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/>

<sup>17</sup> Ibid; The Economist Intelligence Unit (2020) *Methodology: Measuring the prevalence of online violence against women*: [https://cdn.vew.design/private/WbTNqdQVVvgyq5TIBiYpWVmMCJQ2/hyw1xhPZO6\\_EIU\\_METHODODOLOGY\\_PREVALENC\\_E%20OF%20ONLINE%20VIOLENCE%20AGAINST%20WOMEN\\_FINAL.pdf.pdf](https://cdn.vew.design/private/WbTNqdQVVvgyq5TIBiYpWVmMCJQ2/hyw1xhPZO6_EIU_METHODODOLOGY_PREVALENC_E%20OF%20ONLINE%20VIOLENCE%20AGAINST%20WOMEN_FINAL.pdf.pdf)

<sup>18</sup> When looking at terminology related to different types of TFGBV, it is important to be aware that: 1) there are no consistent, standard definitions and methodologies to conceptualize and measure TFGBV; and 2) as digital technologies and virtual applications, tools and platforms rapidly evolve and change, so do the ways that they are used to harass, intimidate and abuse women and girls.

<sup>19</sup> Dunn (2020); Take Back the Tech, Luchadoras and SocialTic, *13 Manifestations of gender-based violence using technology*: <https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology>

Examples include:<sup>20</sup>

- An individual threatening via texts and social media to physically and sexually assault a women's rights activist.
- An armed group threatening via social media to rape women from an opposing political group.
- A trafficker threatening via phone calls and texts to harm a woman if she seeks protection or prosecution through the justice system.

**Harassment:** Unwanted acts that are intrusive, disturbing or threatening perpetrated through phone calls, texts, emails, social media and other online communication applications and platforms, comments sections of websites, etc.<sup>21</sup> Harassment can involve a single targeted misogynistic or sexist comment, including casual sexual harassment in the form of comments on appearance. It commonly also includes more sustained abuse by an individual or a group of harassers. Different tactics may be used, such as **cyberbullying, mobbing, trolling and hate speech** (see Annex 1). Women and girls experience high levels of harassment online and via ICTs,<sup>22</sup> and the harassment is often gendered, sexualized and targeted at other aspects of identity, such as race or sexuality.<sup>23</sup> Harassment includes coordinated and organized attacks against particular women or issues relevant to women or women's rights.<sup>24</sup> Examples include:

- Using sexist or hateful language toward a woman, groups of women or all women on a social media platform.
- Arranging a large scale online negative campaign directed at an LBTIQ+ woman through Twitter.
- Sending unwanted sexually explicit images and messages to a woman or girl via her mobile phone.
- Unrelenting phone calls from an unknown man sexually harassing a woman.

**Stalking**, also called **cyberstalking**: Repeated unwanted monitoring, communication or threatening behavior. It includes monitoring a woman or girl's calls, texts, social media and email, including through installing spyware to monitor activities on a computer or phone, and using GPS technology to track a woman's location.<sup>25</sup> It can also include persistent harassing calls and texts that cause feelings of helplessness, fear and continuous stress. Examples include:

- A perpetrator of intimate partner violence monitoring a survivor's social media accounts, emails, and phone calls and tracking her location as a tactic of control.
- An unknown perpetrator monitoring a woman's rights activist's location and communicating that he knows where she and her children are at different times of the day to instill fear and intimidate her.

**Image-based abuse.** Creating, sharing or threatening to share images of a person without consent.<sup>26</sup> It includes **image-based sexual abuse (IBSA)**, which involves abuse of images that are intimate or of

---

<sup>20</sup> The examples given were provided by people interviewed for this learning series.

<sup>21</sup> Take Back the Tech, Luchadoras and SocialTic: <https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology>

<sup>22</sup> Dunn (2020)

<sup>23</sup> Henry and Powell (2016) Technology-Facilitating Sexual Violence. A Literature Review of Empirical Research, *Trauma Violence Abuse*, 19, 1–14.

<sup>24</sup> Dunn (2020)

<sup>25</sup> APC (2017)

<sup>26</sup> Image-based sexual abuse (IBSA) is sometimes referred to as 'revenge porn'. The term revenge porn is victim-blaming and implies wrong-doing on the part of the victim and implies that the victim was somehow complicit in producing the images. The term image-based sexual abuse is therefore used for this reason. It is also preferred because it recognizes diverse forms the abuse takes and that perpetrators have diverse motivations beyond that of revenge. Added to this, the images might not be pornographic at all, or may not serve the purposes of pornography. For more information see McGlynn, C., Rackley, E., Houghton, R. (2017) 'Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse', *Feminist Legal Studies* (2017) 25:25–46.

a sexual nature, as well as abuse using images that may not be sexual, but may cause harm to a woman or girl. Perpetrators may take or create images without the woman or girl knowing or consenting, or they may have been provided or made consensually, or through pressure or coercion. The images may be sent to the survivors' friends, family and co-workers, shared more widely via text or social media, and/or posted to pornography or other websites. Threats to share images are used to exploit or extort women and girls, with perpetrators threatening to use a sexual image to coerce a woman or girl into providing additional explicit photos, videos, sexual acts or sex, forming or continuing a relationship, engagement in human trafficking, money or other things. Examples include:

- An ex-partner distributing an intimate image via social media to punish a woman for ending a relationship.
- In a conservative community, an acquaintance threatening to publish an image of a woman speaking with a male who is not a member of her family to blackmail her for sex.
- An unknown perpetrator superimposing a woman's face onto pornographic content using deepfake technology and using it to blackmail her.

**Publishing private information.** Sharing private information about a woman or girl online to harass, embarrass and/or harm her reputation. Threats to publish private information may also be used to exploit, extort or coerce a woman or girl. **Doxing** is one form of publication of private information and involves sharing personal information such as address and phone number on the Internet without a woman or girls' consent. It is often done to intimidate a woman by driving online harassment against her and making her fear that she may be harassed or harmed in person. Examples include publishing a woman politician or journalists' contact information via social media or a blogpost and inciting others to intimidate or rape her.

**Impersonation, including catfishing.** The use of digital technology to assume the identity of a person or someone else to access private information, exploit, embarrass, discredit or shame a woman or girl, contact or mislead them, or create fraudulent documents. Examples include creating fake social media accounts and websites to groom and recruit girls and women into sex trafficking.

### *Who is at risk of technology-facilitated gender-based violence?*

All women with access to mobile phones and the Internet are at risk of TFGBV in the same way that all women are at risk of offline GBV. This is due to patriarchal social relations which create and maintain structural gender inequality and discrimination and that subordinate women in relation to men. However, some women are more likely to experience it because of who they are or what they do.<sup>27</sup> Reports show that women with multiple intersectional identities based on race, ethnicity, ability, caste, sexual orientation, gender identity and expression face higher rates of online harassment and attacks.<sup>28</sup> See Box 1 for more information on intersectionality and TFGBV.

#### **Box 1 Intersectionality and TFGBV<sup>29</sup>**

TFGBV is rooted in racism, misogyny, homophobia, transphobia and other forms of discrimination. Depending on a woman's intersecting identity factors, she can be targeted by sexist and misogynistic online attacks, as well as attacks that focus on her race, Indigeneity, sexual orientation, disability, religion, gender identity and gender expression. Intersectionality scholar Patricia Hill Collins (1990) notes that an individual's intersecting social locations cannot be easily separated. How a person experiences sexism will

<sup>27</sup> Amnesty International (2018) *Toxic Twitter*. <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/>; Plan International (2020) *Free to Be Online? Girls' and young women's experiences of online harassment*, The State of the World's Girls Report: <https://plan-international.org/publications/freetobeonline>

<sup>28</sup> Amnesty International (2018); APC (2017); Glitch UK and End Violence Against Women Coalition (2020) *The Ripple Effect: COVID-19 and the Epidemic of Online Abuse*. <https://glitchcharity.co.uk/wp-content/uploads/2021/04/Glitch-The-Ripple-Effect-Report-COVID-19-online-abuse.pdf>

<sup>29</sup> Dunn (2020) p. 16-17.



be inherently tied to other aspects of their identity. A Black lesbian experiences sexist online attacks against her not strictly as a woman, but as a Black lesbian woman. As such, a person's intersecting identity factors will alter the experiences they have online, influencing the qualitative ways they are attacked and the level of violence geared toward them. For example, racialized women and girls are often subjected to more attacks than white women and girls, and attacks against them focus on their race, whereas race is unlikely to be a factor in online attacks against white women.

The intersectional nature of TFGBV is borne out in research that shows that online abuse aimed at racialized and LGBTIQ+ women often combines sexist, racist and homophobic language, and that individuals with intersecting marginalities face higher rates of TFGBV. The US-based Pew Research Center found that online harassment regularly focused on a person's political views, physical appearance, race and gender. LGBTIQ+ people were particularly targeted with harassment for their sexual orientation. A 2012 study by the European Union Agency for Fundamental Rights (2013) found LGBTIQ+ people were harassed and threatened online because of their gender expression and sexual orientation. They were more likely to have their intimate images distributed without their consent. 2020 data gathered by the same agency indicates more than one in five (22%) LGBTIQ+ people had experienced online harassment in the past 12 months, which is higher than the general female population.<sup>30</sup>

Being a woman in public life and visible online makes women a target for abuse perpetrated using technology.<sup>31</sup> Women in public life, such as politicians, journalists and activists are disproportionately targeted for harassment and threats using technology, including coordinated harassment campaigns.<sup>32</sup> Research looking at the intersection of gender and race in the UK and US, found that Black women journalists and politicians were 84% more likely to be the target of hate speech online compared to their white counterparts.<sup>33</sup> Women's rights defenders and activists are also at high risk of experiencing threats of violence via mobile phone calls, text messages and emails. This includes death threats and threats of sexual violence and rape.<sup>34</sup> Women's rights activists have increasingly been subjected to other forms of online harassment during the COVID-19 pandemic, including Zoombombing.<sup>35</sup>

Evidence consistently shows that age is a risk factor for TFGBV, with adolescent girls and young women particularly vulnerable to sexual harassment, abuse and exploitation perpetrated using mobile phones and social media.<sup>36</sup> According to research undertaken across 31 countries, the violence is

---

<sup>30</sup> Lomba, N. Navarra, C. and Fernandes, M. (2021) *Combatting gender-based violence: Cyberviolence*, European Parliamentary Research Service. For further data on the experiences of LGBTIQ+ people in Europe, see European Union Agency for Fundamental Rights (2020) *A long way to go for LGBTI equality*.

[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). See the following publications for further information on the experiences of LGBTIQ people: Powell, A., Scott, A. and Henry, N. (2020) 'Digital harassment and abuse: Experiences of sexuality and gender minority adults', *European Journal of Criminology*, Volume 17, Issue 2: <https://journals.sagepub.com/doi/epub/10.1177/1477370818788006>

<sup>31</sup> Worldwide Web Foundation: <https://webfoundation.org/2020/11/the-impact-of-online-gender-based-violence-on-women-in-public-life/>; Serra Perello, L. (2018) *Online Gender-Based Violence*.

<sup>32</sup> UN Women (2020) *Online Violence Against Women in Asia: A multi-country study*. <https://asiapacific.unwomen.org/-/media/field%20office%20eseasia/docs/publications/2020/12/ap-ict-vawg-report-7dec20.pdf?la=en&vs=4251>; Abdul Aziz, Z. (2017) *Due Diligence and Accountability for Online Violence Against Women*, Due Diligence Project: <http://duediligenceproject.org/resources/>

<sup>33</sup> Amnesty International (2018)

<sup>34</sup> A/HRC/35/9 Report of the United Nations High Commissioner for Human Rights Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective:

<https://www.ohchr.org/EN/Issues/Women/WRGS/Pages/WaystoBridgetheGenderDigital.aspx>; Kvinna till Kvinna (2015) *The hatred against women human rights defenders – online and offline*. <https://www.peacewomen.org/sites/default/files/Fem%20Defenders.pdf>.

<sup>35</sup> <https://www.apc.org/en/blog/feminists-are-building-their-own-technology-organise-where-are-funders>

<sup>36</sup> OSCE (2019) *OSCE-led survey on violence against women: Main report*, Organization for Security and Cooperation in Europe, Vienna; Plan International (2020)

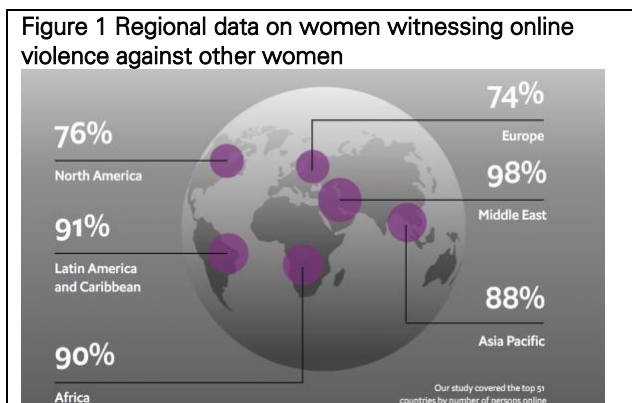
worse for young women who are Black, LGBTQ+, or who have a disability.<sup>37</sup> Risks for online violence and abuse faced by young women may be linked to their high rates of social media use – one study looking at girls experience of online violence found 98% of girls surveyed across 22 countries use social media, with 64% of girls and young women having a high level of usage. It may also be linked to the perception they are more vulnerable, and less confident and knowledgeable.<sup>38</sup> Further research is needed to better understand the particular risks and drivers of various forms of TFGBV faced by different groups of women and girls, particularly displaced, migrant and asylum-seeking women and girls, as there is very little information available on the TFGBV risks and experiences of these women and girls.

## How prevalent is technology-facilitated gender-based violence?

Comparing research findings on TFGBV across settings is challenging as there are no consistent terminology, definitions and measures<sup>39</sup> and studies commonly investigate different things.<sup>40</sup> Further, most of the research on digital violence comes from countries in the global North with low- and middle-income countries in Africa, Asia, and Latin America notably absent from the literature.<sup>41</sup> Additionally, as technology evolves and changes, so does the way it is used to perpetrate GBV, making it difficult to look at trends and changes over time. Despite these challenges, research on TFGBV undertaken with different groups of women and girls across countries confirms that the use of technology to harass, threaten, intimidate, silence, control, exploit and abuse women and girls is pervasive and increasing globally. A 2020 study undertaken by the Economist Intelligence Unit to measure prevalence of online violence against women and girls in 51 countries among adult women with access to the Internet found:<sup>42</sup>

- 38% reported personal experiences with online violence. Younger women aged between 18 and 30 were more likely to have personally experienced online violence, with 45% reporting. This data doesn't include the experiences of adolescent girls.
- 65% reported knowing other women who had been targeted online.
- 85% reported witnessing online violence against other women. There were substantial regional differences in the proportion of women who reported witnessing online violence against other women.<sup>43</sup> See Figure 1 for prevalence of witnessing online violence by region.
- Women in countries with higher levels of gender inequality experience higher levels of online violence.

As shown in Box 2, data from other recent studies investigating TFGBV indicate that it is indeed common, with even higher rates of online violence reported by particular groups of women and girls.



<sup>37</sup> Plan International (2020)

<sup>38</sup> Plan International (2020)

<sup>39</sup> Hinsien et al (2018)

<sup>40</sup> Backe, E., Lilleston, P. and McCleary-Sills, J. (2018) Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence, *Violence and Gender*, Volume 5, Number 3 <https://riselearningnetwork.org/wp-content/uploads/2018/11/vio.2017.0056.pdf>

<sup>41</sup> Ibid

<sup>42</sup> See <https://onlineviolencewomen.eiu.com/>. Note, this research did not include the experiences of girls under the age of 18, or stalking, harassment and threats undertaken using mobile phone calls and texts.

<sup>43</sup> See <https://onlineviolencewomen.eiu.com/> for further data and information from this study, including methodology.

## Box 2. Data on TFGBV among different groups of women and girls

- A study on online violence against **women journalists across 125 countries** found 73% had experienced online violence. The study also found women journalists' disproportionately experience more severe forms of violence than men, and there is a correlation between subjects that women report on and heightened attacks.<sup>44</sup> The reporting theme most often identified in association with heightened attacks was gender (49%), followed by politics and elections (44%), and human rights and social policy (31%).<sup>45</sup>
- A multi-country survey on online violence against **girls and young women** found over half had experienced some form of online harassment. One study carried out across 31 countries with over 14,000 girls and young women found 58% had experienced harassment on social media platforms, with the most common type of online harm abusive and insulting language (reported by 59% of respondents), followed by deliberate embarrassment (41%) as well as body shaming and threats of sexual violence (both 39%). Attacks were most common on Facebook, where 39% have suffered harassment, followed by Instagram (23%), WhatsApp (14%), Snapchat (10%), Twitter (9%) and TikTok (6%).<sup>46</sup>
- A survey of **adult women** in New Zealand, Australia and the UK found 38% had experienced image-based sexual abuse.<sup>47</sup>
- In Pakistan, the Hamara Internet study revealed that 40% of **adult women** had faced various forms of harassment on the Internet.<sup>48</sup>
- In the UK, research found **Black and minorities women and non-binary people** were more likely to experience online abuse during COVID-19 and more likely to report the abuse being worse during the pandemic. Approximately 48% of respondents reported suffering from gender-based abuse, 21% of respondents reported suffering from abuse related to their gender identity and sexual orientation, followed by 18% for their ethnic background, 10% for their religion and 7% for a disability.<sup>49</sup>
- In Uganda, 33% of **adult women** surveyed were found to have experienced online GBV,<sup>50</sup> with the number increasing to 75% among a smaller sample of **women refugees** from the Democratic Republic of Congo, Eritrea, South Sudan and Sudan living in Uganda. These women reported experiencing online abuse, stalking, unwarranted sexual advances and hacking of social media accounts.<sup>51</sup>
- In Serbia, 42% of **women who had been trafficked** reported experiencing digital violence, with 65% exposed to digital threats once they had reported to law enforcement.<sup>52</sup>
- A survey in the US found 97% of **domestic violence support services** reported that abusers use technology to stalk, harass, and control victims. Nearly 80% of programs reported that abusers monitor survivors' social media accounts and 86% reported that victims are harassed through social media.<sup>53</sup>

## How is technology-facilitated gender-based violence manifesting in emergency and fragile contexts?

Digital communications and tools are now considered an integral component of humanitarian response to emergencies. In populations impacted by conflict, disaster and other emergencies,

<sup>44</sup> UNESCO (2020) *Online violence against women journalists: A global snapshot of incidence and impacts*, <https://unesdoc.unesco.org/ark:/48223/pf0000375136>

<sup>45</sup> UNESCO (2021) *The Chilling: Global trends in online violence against women journalists*: <https://en.unesco.org/sites/default/files/the-chilling.pdf>

<sup>46</sup> Plan International (2020)

<sup>47</sup> Powell, A., Fynn, A., Scott, A. Henry, N. (2020) *Image-Based Sexual Abuse: An International Study of Victims and Perpetrators Summary Report*, RMIT University, Goldsmith University, Monash University.

<sup>48</sup> Hamara Internet (2017) *Measuring Pakistani Women's Experiences of Online Violence*, Digital Rights Foundation: <https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf>

<sup>49</sup> Glitch UK and End Violence Against Women Coalition (2020)

<sup>50</sup> Iyer, N., Nyamwire, B. and Nabulega, S. (2020) *Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet*, Pollicy: <https://ogbv.pollicy.org/report.pdf>

<sup>51</sup> Kalemera, A. (2019) *Building Digital Literacy and Security Capacity of Women Refugees in Uganda*: <https://cipesa.org/2019/12/building-digital-literacy-and-security-capacity-of-women-refugees-in-uganda/>

<sup>52</sup> Radoičić, A. (2020) *Behind the screens: Analysis of human trafficking victims' abuse in digital surroundings*, Atina, Belgrade: <http://www.atina.org.rs/en/behind-screens-analysis-human-trafficking-victims-abuse-digital-surroundings>

<sup>53</sup> National Network to End Domestic Violence: <https://nnedv.org/>



mobile phone and Internet use are a lifeline. Refugee, displaced and other emergency-affected women and girls use these tools to communicate with family and friends, seek services and information, and navigate new environments.<sup>54</sup> They enable critical contact with families, help women and girls overcome isolation and feel confident and safe, especially those who are displaced and on the move.<sup>55</sup> Yet, as elsewhere, it is apparent that digital technologies are providing a new set of tools and tactics for perpetrating GBV against women and girls impacted by emergencies. While there is very limited prevalence data from humanitarian contexts, **it is highly likely that TFGBV is occurring at similar or higher rates to non-emergency settings, given the increased vulnerabilities and risks facing women and girls created by conflict, disaster and displacement.**

While TFGBV is understudied in humanitarian contexts, the little data that exists supports this assumption (see data for Uganda in Box 2 for an example), as does information provided by GBV specialists, practitioners and service providers working in diverse emergency-affected settings in the Middle East, Africa and Asia interviewed for this learning series. Due to the sensitivity of the issue, specific informants and contexts have not been cited to preserve confidentiality, security and safety. While the following information does not establish prevalence of TFGBV in humanitarian contexts, and is based on anecdotal information reported by GBV specialists, practitioners and service providers working in emergency-affected settings, it does illustrate different ways that TFGBV is manifesting and the forms of TFGBV that are coming to the attention of GBV practitioners and other humanitarians working with women and girls. It also highlights the pressing need for research and data collection on TFGBV in emergency-affected settings.

Digital technology and ICTs are reported to be commonly used to perpetrate many forms of sexual violence, abuse and exploitation, intimate partner violence, harassment and trafficking of women and girls across humanitarian contexts.<sup>56</sup> Among those perpetrating it are current and former intimate partners, acquaintances within social and community networks, strangers, armed actors, and even humanitarian workers.

### *Sexual harassment, abuse and exploitation*

Across emergency-affected contexts, including those in the Middle East, Asia and Africa, digital technologies are being used to perpetrate sexual harassment, abuse and exploitation of women and girls. IBSA is reportedly a significant problem. Boys and men are creating or obtaining intimate photos of girls and women and sharing or threatening to share them on social media and with the survivors' family. It is understood to be perpetrated to embarrass, shame, punish, manipulate, threaten and blackmail women and girls, with perpetrators sometimes demanding additional intimate images and/or sex in exchange for removing images or refraining from posting further images. Images are being hosted on social media and on websites specifically set up for the purpose of sharing images of girls. In conservative contexts, it is leading to honor crimes, including honor killing.

GBV specialists and services also report pervasive sexual harassment of women and girls perpetrated via text messaging and on social media. Perpetrators are sending women and girls unwanted sexually explicit images (some created using deepfake technology to superimpose women's faces onto pornographic images and video), messages and other unwanted sexual content by email, text and social media. Perpetrators are reported to sexually harass women and girls with the aim of engaging

---

<sup>54</sup> Logie, C. et al (2019) Social ecological factors associated with experiencing violence among urban refugee and displaced adolescent girls and young women in informal settlements in Kampala, Uganda: a cross-sectional study, *Conflict and Health* 13:60: <https://conflictandhealth.biomedcentral.com/track/pdf/10.1186/s13031-019-0242-9.pdf>

<sup>55</sup> Mancini, T., Sibilla, F., Argiropoulos, D. Rossi, M. and Everri, M. (2019) The opportunities and risks of mobile phones for refugees' experience: A scoping review, *Plos One*: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0225684>

<sup>56</sup> Dunn (2020); Simonovic (2018)

in sexual activity, forming a relationship or to extort money or intimate images, with the harassment sometimes escalating to online stalking.

Older adolescents and younger women are being particularly targeted for image-based abuse and ICT-related sexual harassment and stalking. In some humanitarian contexts, online sexual harassment is reported to be perpetrated by younger men known to the woman or girl, whereas in other contexts, perpetrators are reported to be strangers. There are also instances of secondary perpetration by individuals collecting and posting images shared by the initial perpetrator on websites created specifically for the purpose. Technology is also implicated in conflict-related sexual violence against women, with armed groups threatening women from opposing factions with rape and other sexual violence, and using social media and geolocation technology to track, harass and intimidate women who express political views.

Concerningly, ICTs are reportedly being used by humanitarian workers and others in positions of power to sexually harass, abuse and exploit emergency-affected women and girls. These perpetrators are sharing sexually explicit images and persistently messaging and harassing women and girls via phone calls, texts and social media. In some settings, this behavior is reported to be very prevalent. Alarming, and of particular concern, perpetrators are believed to sexually harass girls and young women with whom they have made contact through child-friendly and other protection services. The diversity of experiences, perpetrators and motivations for technology-facilitated sexual harassment and abuse across humanitarian settings makes it clear there is urgent need for context specific assessment and analysis.

### *Intimate partner violence*

There is growing awareness and evidence from research and practice around the world regarding the use of technology in the context of intimate partner violence. ICTs have been linked to physical, sexual, psychological, emotional, and financial abuse in intimate relationships.<sup>57</sup> Yet there remains a scarcity of research on the topic in humanitarian contexts, where rates of IPV often increase. It is therefore highly likely, given its ubiquity in non-humanitarian settings, to be extremely common wherever women and girls have access to ICTs. According to GBV specialists, practitioners and services across emergency settings, perpetrators of IPV are using technology to monitor, stalk, abuse and control their partners. This includes restricting and controlling survivors' access to and use of technology, effectively exerting control over every aspect of a woman's life. This has been exacerbated globally due to social distancing restrictions imposed as part of public health efforts in response to COVID-19, which have meant women's movement and agency have been further controlled and restricted by abusive partners.

### *Trafficking of women and girls*

A commonly neglected issue, human trafficking in emergencies can take many forms including forced prostitution, sexual exploitation, forced marriage, sexual slavery and grooming for extremist and terrorist activities. While there is little information available on TFGBV in the context of trafficking in emergency-affected settings, digital technologies are believed to be used throughout the trafficking cycle to recruit and groom women and girls for sexual exploitation and forced marriage, to transport them, and to maintain control over a woman or girl once she has been trafficked, and even after she has escaped.<sup>58</sup> Recent research undertaken by Serbian NGO, Atina, on prevalence and

---

<sup>57</sup> Duerksen, K and Woodin, E. (2019) Technological intimate partner violence: Exploring technology-related perpetration factors and overlap with in-person intimate partner violence, *Computers in Human Behavior*, V.98: <https://www.sciencedirect.com/science/article/abs/pii/S0747563219301761#:~:text=Cyberstalking%20involves%20behaviors%20such%20as,Chaulk%20and%20Jones%2C%202011%2C%20Watkins>

<sup>58</sup> Anthony, B. (2020) *On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking*, Polaris: [https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-](https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Disrupt-Human-Trafficking)

forms of digital abuse experienced by women and girls trafficked in Serbia, sheds light on the issue of TFGBV in the context of trafficking, finding high prevalence of digital abuse experienced by women and girls prior to, during, and after being trafficked, including as a tactic to intimidate a woman or girl into changing or withdrawing a testimony or statement in criminal proceedings.<sup>59</sup> The use of digital technology in trafficking girls for online sexual exploitation is concerningly prevalent across settings, and the risks for this form of abuse may be particularly high in fragile contexts.<sup>60</sup> Research has also highlighted the role of social media and other Internet platforms in the grooming of women by extremist groups, including for sexual servitude. For example, there is evidence that young women trafficked online to join ISIS ended up in situations of sexual slavery.<sup>61</sup>

Humanitarian agencies and national security services and law enforcement are reportedly ill-prepared to address the issue of TFGBV, with survivors who report or seek help simply advised to change their phone number or social media accounts and profiles. Worse still, when implicated in perpetration of technology-facilitated sexual exploitation and abuse, humanitarian agencies have been said to disbelieve or discredit reporters. This is particularly concerning in light of the proliferation of commitments and initiatives given to addressing sexual exploitation and abuse in humanitarian settings. This is not only inadequate in terms of protecting survivors and preventing further abuse, it also results in making women and girls more vulnerable as they lose access to vital information and services available as part of the humanitarian response.

## Characteristics of TFGBV

Although TFGBV is part of the continuum, and often an extension of in-person violence women and girls face, there are some characteristics that make it different from in-person GBV and that influence how it impacts survivors.<sup>62</sup> Key factors that differentiate online violence from other forms of violence against women include:<sup>63</sup>

- **It can be perpetrated anonymously from anywhere in the world**, across borders and continents, making it very difficult to identify and stop perpetrators or hold them accountable.
- **It can be easily perpetrated** using low-cost technology, limited skill, time and effort.
- **It can be constant**, with a perpetrator having constant access to a survivor through virtual means.
- **It can involve a large number of perpetrators**, including both large numbers of primary perpetrators working together, as well as a large number of secondary perpetrators, such as those who download, forward and share violent or abusive content.
- **It is commonly perpetrated in public spaces**, amplifying the impacts and harms.
- **It can be incredibly difficult to erase or remove abusive content, so it may exist for a long time, and even indefinitely.** Abusive content, such as text and images can be copied and moved to different platforms or sites and be impossible to delete. This can result in ongoing or further victimization or traumatization.

---

[Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf](#)

<sup>59</sup> Radoičić, A. (2020) *Behind the screens: Analysis of human trafficking victims' abuse in digital surroundings*, Atina, Belgrade: <http://www.atina.org.rs/en/behind-screens-analysis-human-trafficking-victims-abuse-digital-surroundings>

<sup>60</sup> See for example, Merten, M. (2020) Tackling online child sexual abuse in the Philippines, *The Lancet* Vol 396; OECD (2020) *Protecting Children Online: An overview of recent developments in legal frameworks and policies*:

<https://www.oecd.org/education/protecting-children-online-9e0e49a9-en.htm>; and OECD (2021) *Children in the Digital Environment: A revised typology of risks*: <https://www.oecd.org/digital/children-in-the-digital-environment-9b8f222e-en.htm>

<sup>61</sup> Jacoby, T. (2015) 'Jihadi brides at the intersections of contemporary feminism', *New Political Science*, 37(4).

<sup>62</sup> Fascendini and Fialová (2011); UN OHCHR (2017)

<sup>63</sup> UN Women (2020) *Online Violence Against Women in Asia: A multi-country study*; The Economist Intelligence Unit (2020)

## Impacts of technology-facilitated gender-based violence on survivors

Concerningly, TFGBV is perceived to be less serious or harmful than other forms of GBV.<sup>64</sup> Yet, GBV perpetrated using ICTs can have profound, long-lasting and severe impacts on a survivor.<sup>65</sup> As with other forms of GBV, the impacts occur on a continuum, accumulate and compound based on a survivor's circumstances, previous experiences and how those around her react and respond.<sup>66</sup> Even a single incident of technology-related abuse, such as a threat of violence on social media or publishing personal information online, can have serious consequences for a woman or girls' physical and mental health and psychosocial well-being.<sup>67</sup> In fact, far from less serious, in some cases, the characteristics of TFGBV identified above can actually amplify the harms and impacts on women and girls, including ongoing traumatization.

Violence perpetrated via technology can lead to acute and long-term mental and emotional stress, distress and illness, including depression and anxiety. Those researching the impacts and working with survivors, report survivors commonly experience a pervasive sense of paranoia and fear linked to the inescapability, perpetuity, permanence and public nature of the abuse. As with in-person physical and sexual violence, IBSA, harassment and threats can violate a survivor's fundamental sense of physical and psychological safety, control and trust in others, leading her to feel constantly in danger. Survivors may lose any sense of safety and trust in others, with the online and offline worlds perceived as constant sources of risk, threat and harm leading to feelings of constant vulnerability. One study undertaken with survivors of IBSA in three high-income countries illuminates the profound interconnected harms linked with IBSA, which researchers termed "social rupture, constancy, existential threat, isolation and constrained liberty."<sup>68</sup> This research highlights the 'endlessness' of this form of violence, with survivors "living each day in 'utter fear' that the images would be (re)discovered. The material was 'out there', beyond their control: constantly available to be shared online, viewed and re-discovered, with each viewing or distribution another iteration of the abuse".<sup>69</sup> In the context of IPV, online stalking and harassment can heighten a survivor's sense of fearfulness and lack of safety and make it very difficult for a survivor to leave a violent relationship or to heal and recover.

The public nature of online violence and social reactions to those targeted can lead to embarrassment, guilt and self-blame which combined with other emotional and psychological impacts can create a sense of hopelessness and helplessness, leading to severe psychological distress, self-harm and even suicide. Incidents of suicide precipitated by digitally perpetrated sexual violence were cited by a number of people interviewed for this learning brief. The reaction of others can be equally devastating. Violence and honor killing have been identified as a direct consequence of IBSA and sexual harassment in a number of settings. The lack of effective response to those who experience IBSA and the ability to identify their location via social media means that even if young women are able to relocate elsewhere, they remain at-risk of honor-based violence. Honor-based violence in response to TFGBV was reported by people interviewed for this learning brief. In conservative communities, survivors of IBSA or other online sexual abuse or harassment live in constant fear of their families and others in the community finding out. This is because similar to other forms of GBV, survivors of technology-facilitated sexual violence are blamed and shamed for the violence due to the stigma and social norms attached to women's bodies and sexuality. The

---

<sup>64</sup> Digital Rights Pakistan (2018); Dunn 2020

<sup>65</sup> McGlynn, C., Johnson, K. and Rackley, E. (2020) 'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse, *Social & Legal Studies* 1–22; Iyer, Nyamwire and Nabulega (2020); APC (2017); Dunn (2020).

<sup>66</sup> Interview with Associate Professor Nicola Henry, RMIT University.

<sup>67</sup> Amnesty reveals alarming impact of online abuse against women (2017):

<https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/>

<sup>68</sup> McGlynn, Johnson and Rackley (2020)

<sup>69</sup> Ibid

serious, and at-times life-threatening impacts of TFGBV, require GBV programs and services to urgently develop capabilities to respond quickly and effectively to address psychological and physical safety threats survivors may face.

In addition to physical and psychological harms, TFGBV can have a host of other negative consequences for survivors. This includes economic impacts, with women losing or leaving employment due to online abuse and harassment, or disengaging from income generating or other economic activities online. See *Learning Brief 3 Implications of technology-facilitated gender-based violence* for more information on wider impacts of TFGBV.

## Priority actions for building knowledge and evidence about TFGBV in emergency contexts

TFGBV is occurring in humanitarian contexts, and it is highly likely that it is occurring at similar or higher rates to non-emergency settings. Yet, little is known about the problem and the specific experiences and risks facing women and girls impacted by conflict, disaster and displacement. While it should always be assumed that women and girls are experiencing TFGBV, there is a pressing need to build and share knowledge, awareness and evidence about the nature, scope and risk factors for TFGBV in and across humanitarian contexts. The following five priority actions are suggested as practical first steps GBV practitioners and specialists can take to help do this.

1. **Build your own and others' knowledge and awareness about TFGBV.** See below for resources to help with this.
2. **Safely include TFGBV in GBV assessments** to learn from and with women and girls and their organizations in your context about:
  - How technology-facilitated abuse and violence is manifesting and impacting women and girls;
  - The specific TFGBV experiences, risks and impacts on different groups of women and girls. This includes displaced, refugee and migrant women, young women, racial, ethnic and religious minority women and girls, women and girls with disability, those with diverse sexual and gender identities, and women's rights activists;
  - Women and girls' solutions to TFGBV and how to support them to implement solutions.
3. **Safely share information generated about TFVGBV** with national and local GBV and women's rights organizations, humanitarian and national decision-makers, donors and other relevant stakeholders.
4. **Advocate with humanitarian and national decision-makers and donors** to direct attention and resources to research and other knowledge-building activities on TFGBV.
5. **Include research, evaluation and other knowledge-generation activities on TFGBV** in GBViE prevention, risk mitigation and prevention programming. Document and share knowledge and evidence generated.

## Resources for learning about TFGBV

This learning brief has provided an introductory overview of the issue of TFGBV, and those working on GBViE in emergencies are encouraged to review additional information, research and resources on the nature, scope and impacts of TFGBV, including those listed below.



- **Measuring the prevalence of online violence against women**, Economist Intelligence Unit, <https://onlineviolencewomen.eiu.com/>
- **Know More, Take Back the Tech**, <https://www.takebackthetech.net/know-more>
- **Manifestations of Technology-related Gender-Based Violence**, GenderIt <https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology>
- **Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective** (2017) <https://digitallibrary.un.org/record/1641160?ln=en#record-files-collapse-header>
- **Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences**, Association for Progressive Communications (2017) <https://www.apc.org/en/pubs/voices-digital-spaces-technology-related-violence>
- **Technology-Facilitated Gender-Based Violence: An Overview**, Dunn, S. (2020) <https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview>
- **Free to Be Online? Girls' and young women's experiences of online harassment**, Plan International (2020) <https://plan-international.org/publications/freetobeonline>
- **Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet**, Iyer, N., Nyamwire, B. and Nabulega, S. (2020) <https://ogbv.policy.org/report.pdf>
- **Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence**, Backe, E., Lilleston, P. and McCleary-Sills, J. (2018) <https://riselearningnetwork.org/wp-content/uploads/2018/11/vio.2017.0056.pdf>
- **Voices from digital spaces: Technology-related violence against women**, Fascendini, F. and Fialová, K. (2011) [https://www.apc.org/sites/default/files/APCWNSP\\_MDG3advocacypaper\\_full\\_2011\\_EN\\_0.pdf](https://www.apc.org/sites/default/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdf)
- **Toxic Twitter**, Amnesty International (2018) <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/>
- **'Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse**, McGlynn, C., Rackley, E., Houghton, R. (2017) *Feminist Legal Studies* <https://link.springer.com/article/10.1007/s10691-017-9343-2>
- **Image-Based Sexual Abuse**, McGlynn, C. and Rackley, R. (2017) *Oxford Journal of Legal Studies*, <https://academic.oup.com/ojls/article-abstract/37/3/534/2965256?redirectedFrom=fulltext>
- **'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse**, McGlynn, C., Johnson, K. and Rackley, E. (2020) *Social & Legal Studies* <https://journals.sagepub.com/doi/full/10.1177/0964663920947791>

## Annex 1 Common technology-related violence terms and definitions

<b>Astrourfing</b>	Dissemination or amplification of content (including abuse) that appears to arise organically at the grassroots level and spread, but is actually coordinated (often using multiple fake accounts) by an individual, interest group, political party, or organization. <sup>70</sup>
<b>Catfishing</b>	When someone pretends to be someone they're not by using social media to create a false identity, usually to defraud or scam someone else. <sup>71</sup>
<b>Data breach</b>	A security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. <sup>72</sup>
<b>Data security</b>	The practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures. <sup>73</sup>
<b>Deepfake</b>	Digital images and audio that are artificially altered or manipulated by AI and/or deep learning to make someone do or say something he or she did not actually do or say. Pictures or videos can be edited to put someone in a compromising position or to have someone make a controversial statement, even though the person did not actually do or say what is shown. Increasingly, it is becoming difficult to distinguish artificially manufactured material from actual videos and images. <sup>74</sup>
<b>Digital technologies</b>	Digital technologies are electronic tools, systems, devices and resources that generate, store or process data. They include the infrastructure, devices, medias, online services and platforms that we use for communication, information, documentation, networking/relation and identity needs. <sup>75</sup>
<b>Documenting or broadcasting sexual assault</b>	Recording and/or disseminating images of sexual assault on social media, via text, or on websites. <sup>76</sup> This is an additional form of sexual violence against the victim-survivor.
<b>Doxing or doxxing</b>	Short for 'dropping docs', a form of publication of private information (see below), that involves sharing personal information such as a person's legal name, address, phone number, contact information, driver's license, workplace, and private documents or correspondence on the Internet without their consent. <sup>77</sup> It is often done with malicious intent to intimidate the person by driving online harassment against them and making them fear that they may be harassed or harmed in person.
<b>Flaming</b>	Flaming is the act of posting or sending offensive messages over the Internet. These messages, called "flames," may be posted within online discussion forums or newsgroups, or sent via e-mail or instant messaging programs. The most common area where flaming takes place is online discussion forums, which are also called bulletin boards. <sup>78</sup>
<b>Hacking</b>	The unauthorized intrusion into a device or network, hacking is often carried out with the intention to attack, harm, or incriminate another

<sup>70</sup> Penn America Online Harassment Field Manual: <https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/#astro>

<sup>71</sup> eSafety Commission Australia: <https://www.esafety.gov.au/young-people/catfishing>

<sup>72</sup> [https://en.wikipedia.org/wiki/Data\\_breach](https://en.wikipedia.org/wiki/Data_breach)

<sup>73</sup> <https://www.ibm.com/topics/data-security>

<sup>74</sup> The Brookings glossary of AI and emerging technologies: <https://www.brookings.edu/blog/techtank/2020/07/13/the-brookings-glossary-of-ai-and-emerging-technologies/>

<sup>75</sup> IGI Global Dictionary: <https://www.igi-global.com/dictionary/digital-technology/7723>

<sup>76</sup> Dunn (2020)

<sup>77</sup> eSafety Commission Australia: <https://www.esafety.gov.au/about-us/tech-trends-and-challenges/doxing>

<sup>78</sup> <https://techterms.com/definition/flaming>

	individual by stealing their data, violating their privacy, or infecting their devices with viruses. <sup>79</sup>
<b>Hate speech</b>	Expression that attacks a specific aspect of a person's identity, such as their race, ethnicity, gender identity, religion, sexual orientation, disability. <sup>80</sup>
<b>Image-based sexual abuse</b>	Includes a wide range of behaviors that involve taking, sharing or threatening to share intimate images without consent. <sup>81</sup> Image-based sexual abuse is sometimes referred to as 'revenge porn'. The term image-based sexual abuse is preferred as it recognizes diverse forms the abuse takes, and that perpetrators have diverse motivations beyond that of revenge. Further, 'pornography' can be understood as implying that the victim was somehow complicit in producing the images. Further, the images might not be pornographic at all, or may not serve the purposes of pornography. <sup>82</sup>
<b>Misinformation and defamation</b>	Spreading fake or exaggerated news through rumors or falsehoods that aim to discredit women, and in particular public figures (for example, public officials, activists, journalists). <sup>83</sup>
<b>Mobbing, also called cybermobbing or networked harassment</b>	Organized and coordinated attacks by a group of people against particular individuals or issues, such as by groups that target feminists or people who post about racial equality issues online. <sup>84</sup>
<b>Online grooming</b>	Involves using the Internet to trick, force or pressure a person into doing something sexual. <sup>85</sup>
<b>Online stalking</b>	The repeated harassment of individuals, perpetrated by means of mobile phones or messaging applications, in the form of crank calls or private conversations on online applications or in online chat groups. <sup>86</sup>
<b>Online sexual harassment</b>	Refers to any form of online unwanted verbal or non-verbal conduct of a sexual nature. It includes sending unwelcome sexual requests, comments and content.
<b>Sextortion</b>	Sexual extortion, or 'sextortion' occurs when an individual has, or claims to have, a sexual image of another person and uses it to coerce a person into doing something they do not want to do. <sup>87</sup>
<b>Social media</b>	Social media is a collective term for websites and applications which focus on communication, community-based input, interaction, content-sharing and collaboration. Forums, microblogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media. <sup>88</sup> Social media is Internet-based and gives users quick electronic communication of content. Content includes personal information, documents, videos, and photos. Users engage with social media via a computer, tablet, or smartphone via web-based software or applications. The most commonly used social media platforms are: <ol style="list-style-type: none"> <li>1. Facebook (2.74 billion users)</li> <li>2. YouTube (2.29 billion users)</li> <li>3. WhatsApp (2 billion users)</li> <li>4. Facebook Messenger (1.3 billion users)</li> <li>5. Instagram (1.22 billion users)</li> <li>6. Whatsapp (1.21 billion users)</li> <li>7. TikTok (689 million users).<sup>89</sup></li> </ol>

<sup>79</sup> Pen America Online Harassment Field Manual: <https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/#hacking>

<sup>80</sup> Ibid

<sup>81</sup> McGlynn, C., Rackley, E., Houghton, R. (2017) 'Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse', *Feminist Legal Studies* (2017) 25:25–46

<sup>82</sup> Ibid

<sup>83</sup> Economist Intelligence Unit (2020)

<sup>84</sup> Dunn (2020)

<sup>85</sup> ChildLine UK: <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-grooming/>

<sup>86</sup> See Gendering Surveillance: <https://genderingsurveillance.internetdemocracy.in/>.

<sup>87</sup> Dunn (2020)

<sup>88</sup> TechTarget Network: <https://whatis.techtarget.com/definition/social-media>

<sup>89</sup> Investopedia: <https://www.investopedia.com/terms/s/social-media.asp>

<b>Synthetic sexual media</b>	The manipulation of images, making it appear as though people are engaging in sexual activity they did not engage in. Synthetic sexual media may be produced for sexual entertainment and profit, to harass women and purposely cause them harm. It can include using software to superimpose a person's face onto a sexual image. Deepfakes are a form of synthetic social media. <sup>90</sup>
<b>Trolling</b>	Trolling is when a user abuses or harasses others online for 'fun'. Trolls deliberately post comments or message, upload images or videos and create of hashtags for the purpose of annoying, provoking or inciting violence against women and girls. <sup>91</sup> Many trolls are anonymous and use false accounts.
<b>Zoom-bombing</b>	Occurs when people join online meetings or gatherings in order to post racist, sexist, pornographic or anti-Semitic content to shock and disturb viewers, is a form of networked harassment. <sup>92</sup>

### *The GBV AoR Help Desk*

*The GBV AoR Helpdesk is a unique research and technical advice service which aims to inspire and support humanitarian actors to help prevent, mitigate and respond to violence against women and girls in emergencies. Managed by Social Development Direct, the GBV AoR Helpdesk is staffed by a global roster of senior Gender and GBV Experts who are on standby to help guide frontline humanitarian actors on GBV prevention, risk mitigation and response measures in line with international standards, guidelines and best practice. Views or opinions expressed in GBV AoR Helpdesk Products do not necessarily reflect those of all members of the GBV AoR, nor of all the experts of SDDirect's Helpdesk roster.*

### The GBV AoR Helpdesk

You can contact the GBV AoR Helpdesk by emailing us at: [enquiries@gbviehelpdesk.org.uk](mailto:enquiries@gbviehelpdesk.org.uk)

The Helpdesk is available 09.00 to 17.30 GMT Monday to Friday.

Our services are free and

<sup>90</sup> Dunn (2020)

<sup>91</sup> eSafety Commission Australia: <https://www.esafety.gov.au/women/online-abuse-targeting-women>

<sup>92</sup> Dunn (2020)