TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE IN ASIA

BANGLADESH
PROJECT BACKGROUND

Funded by USAID, NORC at the University of Chicago and the International Center for Research on Women (ICRW) set out to assess technology-facilitated gender-based violence (GBV) in Bangladesh, including trends; programs and policies currently working to prevent, mitigate and respond to this form of violence; and gaps and recommendations for future programming. To inform this case study, the team utilized existing literature and relied on key informant interviews with leaders of NGOs and researchers working on the topic in Bangladesh.

KEY FINDINGS

OVERVIEW

Bangladesh has seen a rapid rise in Information Communication Technology (ICT) infrastructure and usage over the last ten years,7 and, in turn, increasing prevalence of technology-facilitated GBV. Populations disproportionately impacted by this type of violence reflect those generally marginalized by Bangladeshi society, including women and girls, ethnic and religious minorities, and members of the LGBTQI+ community. While there are legal frameworks and programs currently in place to address the issue of technology-facilitated GBV, there are notable gaps and barriers to implementation such as a lack of awareness on this issue and the need for increased capacity to prevent and respond to violence in the form of technology-facilitated GBV.

KEY TERMS AND CONCEPTS

- **Technology-facilitated gender-based violence (GBV)** is any action carried out using the internet and/or mobile technology that harms others based on their sexual or gender identity or by enforcing harmful gender norms.1
- **Cyber harassment** can be broadly understood as repeated online behaviors or expressions targeted at a particular person or group with intent to cause them distress.2
- **Cyberstalking** is a severe form of cyber harassment that constitutes a credible threat of harm to the target.3
- **Image-based abuse** encompasses nonconsensual distribution and creation of private and/or sexual images including the recording of sexual assaults, as well as threatening to do so.4
- **Non-consensual distribution of intimate images** refers to the distribution of private or sexually explicit images or videos of individuals without their consent.5
- **Deepfakes** are images, audio, and/or video that are created using a form of artificial intelligence to appear real, which can be used to superimpose an individual's face to videos or images to create fake pornography. When these are created, distributed, or threatened to be distributed without the consent of the person whose face appears, it is considered a form of image-based abuse.6

---

3 ibid
PREVALENCE, PERPETRATION, AND MOTIVATION

In 2017, it was reported that 73 percent of women internet users in Bangladesh had experienced cybercrimes.8 One key form of technology-facilitated GBV that is prevalent in Bangladesh is cyber harassment, which includes cyberstalking. It is important to note that contextual issues around what constitutes harassment vary according to regional and cultural contexts. For example, while some instances of cyber harassment can clearly be identified as acts of GBV across all contexts due to its intentional and repetitive nature, other instances such as general sexual content in communications and sexually explicit messages (e.g. calling a woman “sexy” or “hot”) which may be normalized in some contexts, are perceived as severe sexual harassment in Bangladesh. Moreover, there is a perception that violence or harassment perpetrated online is not taken as seriously as reports of physical or in-person violence. However, those experiencing this form of violence can suffer significant psychosocial and economic impacts.9 Further, in many instances, there is a clear connection between online and offline violence where perpetrators escalate from online violence to physical and sexual violence.10

Key informant discussions indicate that image-based abuse is another prevalent form of technology-facilitated GBV in Bangladesh, including non-consensual distribution of intimate images and the non-consensual creation of sexual imagery. Some examples of this in Bangladesh include students exchanging such content in school, the non-consensual distribution of private images by current or ex-intimate partners, the sharing of non-consensual images by third parties with no relation to the target with the intent to blackmail (commonly referred to as “sextortion”), and the creation and sharing of degrading deepfakes.

In 2020, nation-wide protests erupted in Bangladesh when a video of a group of men sexually assaulting a woman went viral, which in turn led to further cyber harassment of women protesters and brought the issue of GBV, and particularly technology-facilitated GBV, to the forefront of national dialogue.11 This highlights the role of technology and social media in supporting an environment where perpetrators feel comfortable and are easily able to share such horrifying acts with a wide audience. Not only does the non-consensual sharing of the assault re-victimize survivors and their families, but, in the absence of well-defined and well-enforced legal actions, these platforms facilitate the perpetuation of technology-facilitated GBV and the silencing of survivor voices.

Societal norms and conflicts that occur offline are often also reflected online, particularly in reference to marginalized populations. Women and girls in Bangladesh are disproportionately targeted by GBV, and the contexts surrounding the violence they face can be just as varied online as they are offline. Women who are politically active face especially degrading and humiliating comments and harassment online. To understand such violence against women in the political sphere, it is important to recognize the larger political landscape in Bangladesh. While both the Prime Minister and the Leader of the Opposition are women, government ministries, particularly elected officials, are largely comprised of

---

men. These gender dynamics feed into an overall patriarchal political environment which can transmit to the nature of public discourse surrounding politics. Perpetrators who believe that political power and authority should be held by men and feel threatened by vocal or politically active women, feel motivated to attack or harass those women online to undermine their qualifications or authority.

For those not in the public view, it is common for perpetrators who are men to have some sort of relationship with the women targets, whether they are a current or previous intimate partner, someone who has faced romantic rejection, a classmate, colleague, or even family members who may be trying to police or shame a woman’s behavior.

Perpetrators may also target populations who have been historically marginalized or disenfranchised. In Bangladesh, this can include ethnic and religious minorities, and identifying, or being perceived as, a member of the LGBTQI+ community, especially Hijras: an identity category in Bangladesh for people assigned male at birth who develop a feminine gender identity and prefer to be recognized as third gender. In considering these factors, experts in the field emphasize the importance of intersectionality. For example, even within ethnic minority communities including those from the Chittagong Hill Tracts (CHT), researchers found that women belonging to these communities do not feel comfortable seeking support from traditional leaders, who are usually men, as they feel the leaders will believe or protect men perpetrators. In another instance, researchers studying technology-facilitated GBV experienced by Hijras emphasized that, as cis-gendered women, they had to spend considerable time in building trust and relationships with the Hijra community in order to speak with them, as Hijras have been ostracized and condemned by both men and women in Bangladesh. With regard to marginalization due to sexuality, Section 377 of the colonial penal code still exists in Bangladesh, outlawing any sexual behavior “against the order of nature…” Thus, not only are LGBTQI+ members disproportionately targeted by harassment, but they also often do not seek support as it is dangerous for their sexuality status to be outed to the government and public.

**PREVENTION, MITIGATION, AND RESPONSE**

GBV has lately been at the forefront of national discussion in Bangladesh usually focusing on the topics of child marriage, rape, and other acts of violence against women. However, recent measures taken by the government, NGOs, and researchers indicates that technology-facilitated GBV is also gaining national recognition and is seen an issue that warrants policy and programmatic action. For example, as part of a study on Sexual and Reproductive Health by BRAC University, the Digital Sister project is creating videos focused on raising community awareness about cyber harassment in Bangladesh. The International Foundation for Electoral Systems (IFES) have outlined their recommendations on the topic based on their 2019 study of online violence against politically and civically engaged women in Bangladesh. The

---


13 The Chittagong Hill Tracts (CHT) is a south-eastern part of Bangladesh that is home to eleven indigenous ethnic groups that are distinct from the majority Bengali people of Bangladesh in respect of race, language, culture, heritage, religion, political history, and economy. (Unrepresented Nations and Peoples Organization, 2018)

Bangladesh Legal Aid Services Trust (BLAST) has also assessed Bangladesh’s current laws, identified limitations and gaps, and made recommendations to address cyber violence against girls. 

To provide support to GBV survivors of all kinds, the Ministry of Women and Children Affairs established several “One Stop Crisis Centers” (OCC) to provide medical, legal, and social services. To penalize preparators, the existing legal framework currently addresses general harassment and defamation within the pre-colonial penal code as well as post-independence laws. Specific to cybercrime, Bangladesh passed the Information Communication Technology Act in 2006, and passed an amendment act in 2013 that established a Cyber Crimes Tribunal that addresses cases of cyberviolence. In 2018, Bangladesh passed the Digital Security Act of 2018 to curb violent extremism and hate speech online. In 2020, Bangladesh established an all-woman police unit specifically to address cyber-crimes against women.

GAPS AND RECOMMENDATIONS

While there have been several civil society and government actions to address the issue of technology-facilitated GBV in Bangladesh, some key gaps in policy and programming remain.

- **Strengthen legal protection mechanisms:** While current laws and frameworks exist in theory to protect against technology-facilitated GBV, there are gaps in proper implementation. The Digital Security Act of 2018 was initially put into place to address hate speech; however, it has been described by many as draconian and used by the government to suppress dissent and target free speech. It is not regarded by the public as a protection mechanism. Other laws and frameworks contain ambiguities that make it difficult to prosecute cases of cyberviolence. A recommendation is to provide resources and training to legal actors in the field to establish concrete procedures on how the existing legal frameworks can be applied to prosecute cases of technology-facilitated GBV and assess whether new laws need to be established.

- **Increase survivor-centric resources and support:** It is reported that around 90 percent of instances of online violence are not reported by victims. While crisis centers for GBV exist, there are none specific to online violence. Combined with the general lack of information around the issue, survivors often feel they will not be taken seriously if they seek support. Similarly, while dedicated police units exist for cybercrimes, it has been reported that often “no one is there at the desk,” or when they are, they do not provide a supportive environment where survivors or their families feel safe. Thus, victims and their families do not always feel comfortable utilizing this support from the police or other existing frameworks, which in turn reduces both reporting and prosecution. Additionally, because section 377 of the Penal Code of Bangladesh still exists, members of the LGBTQI+ community do not feel protected or seek support for fear of outing. Comprehensive and sufficient resources, such as access to legal support and therapy services, are essential for survivors. Additional training on trauma-informed approaches for police and prosecutors is needed to mitigate re-victimization and re-traumatization of survivors when they seek support. While funding for these resources is seen

---

as a formidable challenge, additional funding from the national government and international donors can enhance survivor-centric resources and efforts.

- **Improve coordination between private and public sector:** There is limited data provided by both the government and private technology companies to inform further research and programs to address technology-facilitated GBV. Additionally, security and privacy guidelines by large social media platforms are often not well-understood by or adapted for Bangladeshi users. Flagging or deleting harmful content that is in Bengali has also been more difficult than content in English. The government of Bangladesh and private technology companies must coordinate and cooperate to address the technological environment that facilitates and perpetuates GBV.

- **Introduce social and behavioral change programming:** As stated above, there is a general lack of understanding of technology-facilitated GBV in Bangladesh, and its impacts are often trivialized by the public. Additionally, because of existing societal norms and taboos surrounding sex and sexuality in general, survivors often fear “reputational damage” that not only affects them but also their family and friends, which further discourages reporting of cybercrimes. While the ICT sector has grown rapidly in Bangladesh, a similar growth has not been seen in programs and efforts to educate ICT users on safety and privacy best practices. “Cyber hygiene” trainings in schools can help educate users about digital security, while general awareness raising campaigns can help reduce the general stigma surrounding gender-based violence.

---

**Recommended citation:** NORC at the University of Chicago and the International Center for Research on Women. (2022). Case Study: Technology-facilitated Gender Based Violence in Bangladesh.