How Can We Protect Women and Youth from Cyber Violence?

UNDP, in collaboration with The Daily Star, organised a roundtable titled "Scanning the Horizon: Addressing Cyber Violence against Women and Youth through Policy and Awareness" on November 25, 2024. Here we publish a summary of the discussion.

Shahreen Tilottoma, *Project Analyst, UNDP Bangladesh (Keynote Presentation)*

UNDP's project, "SDG Partnership on Combating Cyber Violence against Women," is a joint initiative implemented by UNDP Bangladesh and the UNDP Seoul Policy Centre, with support from the Korean Government. A dedicated team from the Bangladesh Police Cyber Support for Women serves as an implementing partner. This team has undertaken extensive campaigns and capacity-building efforts. Over the past two years, we have focused on three major areas: research and advocacy, legal framework reviews, and communication campaigns.

UNDP actively participated in the global campaign "16 Days of Activism Against Gender-Based Violence" (25 November to 10 December), with this year's theme being "No Excuse: End Violence against Women."

Additionally, we launched the "Be Cyber Smart" campaign, targeting cyber-smart women. This initiative features static posts, animated videos, comics, and a cyber safety toolkit available on UNDP's social media platforms and website.

We launched a film contest titled 'CyberLens' to foster public engagement through creativity. Furthermore, an interactive video, "Screen-er Arale," was developed in collaboration with UN Women. As the first of its kind in Bangladesh, this tool allows viewers to explore scenarios where women can protect themselves from cyber violence or learn prevention strategies.

A training module is under development to enhance police capacities as first responders. We also engaged women entrepreneurs involved in online transactions, e-commerce, and f-commerce to raise awareness and address challenges they face in the digital sphere.

Sheikh Rashedul Islam, *Technology and Cyber Security Specialist*

Data collection is critical in cybersecurity. Effective data modelling ensures that only measurable elements become visible and visible elements can be monitored and improved. This underscores the importance of not only collecting data but also hosting, using, and sharing it effectively across agencies and sectors, including financial institutions.

Cybersecurity is a highly technical field that demands skilled expertise. Many agencies face challenges with unfamiliar tools sourced internationally, lacking the requisite expertise to operationalise them effectively. To address these challenges, agencies must invest in expert guidance, create awareness, and establish robust baseline security measures.

Qadaruddin Shishir, *Fact Check Editor, AFP*

Misinformation and disinformation targeting women in cyberspace manifest in distinct patterns. First, political campaigns, particularly during elections between 2018 and 2024, frequently exploited women's identities to spread disinformation. Women were associated with opposition leaders, with manipulated photos and videos portraying them negatively.

Second, women's identities—especially those of celebrities—are commodified for economic purposes through manipulative content, distorted images, or altered voices, often for financial gain. To combat such crimes, digital and media literacy are crucial for identifying false content.

Sadat Rahman, *Founder, CyberTeens & Winner, International Children's Peace Prize*

Youth and children are among the primary groups facing challenges in cyberspace. While they previously avoided approaching law enforcement for assistance, they are now increasingly compelled to do so. However, youth-led initiatives requires active support from law enforcement agencies and organisations committed to ensuring cybersecurity.

At CyberTeens, where we have been working with teenagers for five years, we have observed a lack of substantial support from law enforcement. Technological advancements are also urgently needed. For instance, cybersecurity-related complaints cannot yet be filed online.

Government and law enforcement agencies must enhance their capacities and develop strategies to engage youth ambassadors actively.

Sharmin Ahmed, *Senior Vice President, Mutual Trust Bank*

Only 30% of bank accounts at our institution are held by women, with just 2,500 belonging to female entrepreneurs. Many fall victim to fraudulent schemes, such as fake business proposals or phishing, leading to financial losses or blackmail after sharing personal information.

Public-private partnerships (PPPs) involving banks, NGOs, and organisations like UNDP can educate women on digital safety. NGOs can advocate for digital literacy, particularly in rural areas, while ensuring victims know where to report incidents and are assured of confidentiality to overcome social stigma.

Faisal Bin Majid, *Research Analyst, UNDP*

In this digital era, our privacy is profoundly disrupted by the rapid rise of AI and apps among people from all walks of life. The immediate concern lies in the spread of nudity, offensive fake videos, and the frequent leaks and circulation of content often targeting gender, which can incite violence. To combat online bullying, retreating from the digital space or assuming that harassment will naturally diminish over time is not a viable solution.

Shoeb Abdullah, *Fact-checker, Disinformation Researcher, Digital Rights Activist*

Violence in cyberspace is disproportionately distributed, with a significant emphasis on gender-based issues. There is a lack of clearly defined discourse on cyber-based gender violence.

Moreover, digital literacy initiatives are frequently proposed without prior assessment or contextual understanding. Women require tailored digital literacy programmes, prompting us to develop a specialised toolkit aimed at preventing harassment and digital violence. Sustained campaigns and awareness efforts focusing on digital literacy are essential to mitigate the growing threat of digital violence.

Zulker Naeen, *Research Coordinator, FactWatch, ULAB*

A recent study titled Cyber Safe and Positive Teens in Bangladesh revealed that only 20% of abuse victims were willing to seek help through formal legal channels, leaving a staggering 80% unwilling to report their experiences.

Rather than adopting a top-down approach, grassroots engagement must be prioritised to effectively prevent cybercrime. Communities should take the lead in designing and implementing programmes tailored to their specific needs and challenges.

Tasnuva Shelley, *Barrister, Supreme Court Bangladesh*

The legal framework for preventing cybercrime is often vague and inconsistent. In many instances, judges and lawyers fail to adequately address cases, resulting in the dismissal of 80% to 90% of them. This highlights a critical gap in the judicial process.

Much like medical professionals, we urgently need digital forensic experts to investigate and unravel digital fraud and cybercrimes effectively. Their expertise could play a pivotal role in ensuring such cases are prosecuted successfully, fostering greater accountability and justice in the digital realm.

Tazkia Labeeba Karim, *Senior Associate, Syed Ishtiaq Ahmed & Associates Law Consultants and Legal Practitioners*

Laws such as the ICT Act and the Pornography Act address issues related to sexual harassment. However, these legal frameworks lack a clearly defined and jurisdictionally robust discourse, hindering the effective prevention of cybercrime.

The reliance on the 1860 Penal Code to address modern digital challenges exacerbates this problem. While changes to the Evidence Act have been made, they remain insufficient for addressing emerging challenges like deepfakes—both an advanced and alarming concept.

While the law addresses defamation, threats, violence, or humiliation, it does not adequately cover these subtler yet impactful forms of harm.

Manisha Biswas, *Programme Coordinator, BLAST*

Since 2023, BLAST has been actively addressing online violence through the formation of the Cyber Support for Women and Children (CSWC) coalition, comprising over 12 organisations, including a dedicated cybercrime team. FIRs filed at the local level often contain inaccuracies in the initial stages due to insufficient sensitisation and specialised training in combating cybercrimes. Ensuring law enforcement personnel receive consistent and comprehensive training is crucial. This must be an ongoing effort, not a one-time measure, to build their capacity effectively. Given the overburdened state of law enforcement agencies, specific directives and resources should be allocated to handle cybercrime cases.

Sharbana Datta, *Project Manager, UN Women*

Online platforms have become sites for various forms of violence, including harassment, bullying, and exploitation, particularly targeting women, marginalised groups, and persons with disabilities. Women with disabilities face compounded challenges, including financial abuse.

To tackle these issues, comprehensive toolkits tailored to address the unique nature of online violence are essential. A centralised website offering information, guidelines, and actionable steps—such as dos and don'ts for individuals—could be an effective first step. A single law is insufficient to address the complexities of technology-based violence. A multifaceted approach is required, combining individual awareness with institutional strengthening.

Rijve Arefin, *Founder, Awareness 360*

In our country, opinions about girls and women often disregard the fact that they have their own lives and autonomy. This becomes especially evident on social media, where any negative news about women, particularly from grassroots and middle-class sections, triggers an avalanche of comments.

When discussing women's empowerment or related issues, these are often dismissed as "women's issues," but in reality, they are fundamental human rights concerns. Addressing this requires educating young boys and men, starting within families and grassroots communities, with targeted lessons on equality, equity, and feminism. While creating toolkits, comics, and graphic novels is valuable, these resources must be localised to resonate with grassroots communities.

Md Golam Sarwar, *Assistant Professor of Law, Dhaka University*

Over the past two decades, numerous laws have been enacted to address issues related to women. However, there remains a lack of implementation or minimal enforcement. The primary reason is that, despite the significant increase in women's participation on online platforms, their engagement is still shaped by unequal power dynamics in society. Until we address these power imbalances, true engagement will remain unattainable.

In terms of gender equality, Bangladesh is a top performer in South Asia, but the ground reality often contradicts this claim. What we see is more symbolic empowerment rather than actual, substantive empowerment of women.

Rezwanul Islam, *Regional Editor, Global Voices*

In Asia-Pacific countries such as India, Malaysia, and the Philippines, laws addressing gender-based violence extend to women, youth, and children. However, in our country, laws are often enacted without sufficient consultation. While we tend to take a more lenient approach, achieving digital hygiene requires investment.

Many people acquire phones without understanding the responsible use. For instance, an Android phone requires an email ID, which is sometimes registered under someone else's name instead of the user's.

Digital violence against women is common here, due to the lack of institutional oversight, unlike in other countries where institutions are highly active in combating such crimes. For example, organisations seeking funding are often asked if they have a sexual harassment policy. To ensure the safety and protection of women, we must take similar steps; otherwise, women will continue to face increasing harassment.

Shahriar Babla, *Consultant, UNDP*

For individuals in urban areas without formal education, content consumption extends beyond platforms like Facebook, YouTube, or LinkedIn; they primarily use TikTok, Likee, and similar applications. We must collaborate with these platforms to establish guidelines tailored to our local context to ensure effective content regulation. Without such measures, policies would remain ineffective.

Behavioural change is critical, as societal norms often fail to recognise or accept diverse identities. This issue extends to platforms like Facebook, where digital advocacy alone cannot resolve systemic biases. A comprehensive approach is required, focusing on education, curriculum reform, and fostering inclusive mindsets from an early age.

Maliha Tabassum, *Assistant Professor, Department of Mass Communication and Journalism, Bangladesh University of Professionals (BUP)*

International standards for addressing cyber violence are not always applicable to Bangladesh, as issues such as intersectionality, societal dynamics, and cultural nuances remain underrepresented.

Furthermore, government efforts to support victims—such as counselling and rehabilitation services—are significantly lacking. This gap has been highlighted in both national and international reports.

ICT teachers must be trained to educate vulnerable, victimised youths (e.g., aged 18–30). There are many cases where victims are turned away by the police and even blamed. This is deeply unfortunate as it discourages both past and future victims from seeking societal guidance. NGOs have attempted to highlight underreported cases, and their initiatives must be supported.

Jyotirmoy Barua, *Advocate, Supreme Court of Bangladesh*

The Cyber Tribunal plays a crucial role in addressing gender-based violence but operates within a limited scope, enforcing legal rights only after societal norms have been violated.

The evolution of Bangladesh's cyber laws reveals significant gaps. Although the oppressive Digital Security Act (2018) was repealed, its successor, the Cyber Security Act (2023), remains authoritarian and lacks provisions for globally recognised cyber offences. Effective criminal law demands clear definitions of offences and penalties, which are currently absent from the legal framework.

Outside the legal system, safeguarding measures remain inadequate. Bangladesh lacks the necessary legal framework to address critical issues such as mental trauma. In the absence of comprehensive regulations, the public remains vulnerable to police harassment.

Anowarul Haq, *Assistant Resident Representative, UNDP*

In Bangladesh, the legal framework often lacks clarity, particularly on penalties, underscoring the need for a robust, specialised framework. Protection mechanisms for vulnerable groups, particularly women, girls, and youths, must be prioritised.

Digitalisation has brought global challenges that require cohesive legislation incorporating regional and international experiences. Legislative amendments must be accompanied by strengthened institutional capacities within law enforcement agencies. For example, units such as the CT-Cyber Crime Investigation (DMP) need advanced resources to address growing backlogs. Establishing dedicated cybercrime units in every division and introducing role-specific training, including gender-sensitive and technologically skilled officers, are essential steps.

Tanjim Ferdous, *In-Charge, NGOs & Foreign Missions, The Daily Star (Moderator)*

This roundtable is an important part of the '16 Days of Activism.' Today's discussion focuses on cybercrime and online violence, which are significant challenges in the modern world. Their impact extends beyond the digital sphere to individual well-being, social dynamics, and psychological health. Women and youth, in particular, are especially vulnerable to the security risks associated with online threats. This discussion aims to raise awareness and explore practical solutions.

RECOMMENDATIONS

- Collecting, hosting, using, and sharing data effectively across agencies and sectors is crucial for cybersecurity.
- Establish dedicated cybercrime units in each division and provide role-specific training, including gender-sensitive and tech-skilled officers.
- Update the legal framework to address contemporary cybercrimes and emerging challenges, such as deepfakes.
- Ensure meaningful youth involvement in cybersecurity efforts
- Prioritise grassroots engagement in preventing cybercrime by empowering communities to design and implement programmes tailored to their specific needs.
- Specialised training for law enforcement agencies is necessary to trace harassers and handle cyber-related complaints.
- Encourage public-private partnerships (PPPs) to raise awareness about digital safety for women, involving banks, NGOs, and organisations like UNDP.
- Enhance digital literacy and ensure individuals are informed of confidential reporting mechanisms.
- Urgently train and deploy digital forensic experts to effectively investigate and prosecute digital fraud and cybercrimes
- Establish an integrated helpline for streamlined support on cyber issues.
- Integrate digital literacy into the national curriculum.