16 DAYS OF ACTIVISM AGAINST GENDER-BASED VIOLENCE

WOMEN AND LAW

Cyber harassment against women and our legal shortcomings

Bangladesh requires an institutional overhaul. The cyber units should be well-trained in digital forensics, gender sensitivity, and victim-centered approaches. The courts should be trained on various novel kinds of digital crimes and harms. Workplaces and educational institutions should come up with systemic and sustainable measures that can assist electronic harassment victims.

FARJANA YESMIN

A case was recently filed under the Cyber Security Ordinance 2025 after a manipulated image of a female faculty member of the University of Dhaka had been posted on the internet with derogatory captions and remarks. This incident pointed towards the invasive abuse of image-manipulation technologies and digital defamation as novel weapons of sexual harassment. Online sexual harassment, launched in particular against women continue to be reported nationwide. These are not isolated cases; these are the symptoms of an escalating crisis of the digital spaces and tools being weaponised against women.

Notably, the online spaces are but continuation and replication of our offline structures, and one of the most evident categories to understand this is gender. Women who engage in the public life, be it in politics, journalism, entertainment or activism, are sexually abused online to ensure that they or are "taught a lesson". Such kinds of digital gender violence compromise the process of democracy, liberty of expression and people's rights and security.

Several legal provisions provisions have been enacted in Bangladesh that target the up-and-coming challenges in the sphere of cyber security and in controlling criminal actions in digital space. For example, the otherwise problematic Digital Security Act 2018 had made it a criminal offence to publish offensive, false or defamatory digital material under sections 25 and 29. Moreover, it had criminalised speeches that call for enmity among classes or communities, or unrest under section 31. However, it was criticised for being poorly drafted and due to its potential ability to curtail freedom of speech. Subsequently, it was replaced with the Cyber Security Act 2023, which brought some minor changes by introducing lesser degrees of punishment and more bailable offences.

Finally, the Cyber Protection Ordinance 2025 replaced the CSA with a more reform-oriented approach towards dealing with the digital space and cyber security issues. It enshrines the right to access the internet, punishment for cyber harassment of women and children, and also criminalises harmful or intimidating materials generated or edited by AI. The law, nevertheless, continues to be critiqued for its ambiguous language, absence of independent oversight by regulatory organisations, and for potentially being open to political abuse.

Besides the cyber laws, criminal laws in general also are relevant, although not effective, in this context. The Penal Code 1860, under sections 354 and 509, deal with offences that infringe the "modesty of a woman". However, the Code, being a colonial-era law, is not as such directly applicable to digital abuse and its provisions can only be made applicable through a wider interpretation.

The Prevention of Women and Children Repression Act 2000 intends to save women and children against physical, sexual and psychological abuse. The law has prescribed harsh penalties and quite commendable victim-responsive approaches. Although the provisions offer somewhat effective solutions concerning traditional kinds of abuse and gender-related violence, its stipulations were not framed keeping the digital space in mind. Section 8 of the Pornography Control Act 2012 deals with various kinds of cybercrimes against women. However, it mostly focuses on punishment but not on protection of survivors. Indeed, the absence of a rights-based approach towards the victim further aggravate its loopholes.

Indeed, we have many laws; but in practice, they are rarely enforced. There is a lack of trained officers in digital crime investigation, as well as a lack of forensic tools and victim-sensitive procedures. When it comes to gender-based harassment, a victim tends to fear humiliation and further harassment. Therefore, most women do not report such incidents considering justice will be served slow or not at all. This particularly applies to women who face gender-based threats, including sexual abuse, rape threats, or non-consensual circulation of images. The Police Cyber Support for Women is a move in the right direction, but its scope and capabilities are far too limited compared to the issue at hand. Furthermore, the specific nature of gender-based digital violence, as has been set out above, is not fully acknowledged in our policy-legal landscape.

While the existing laws have to be streamlined acknowledging the nuances of online sexual harassment and other digital gender-based violence. Pertinently, digital violence based on gender must be spelt out not as an add-on to the general provisions. Threats that are serious should receive criminal penalties, whereas other cases should receive greater civil redress, including compensation, and administrative penalties.

Bangladesh also requires an institutional overhaul. The cyber units should be well-trained in digital forensics, gender sensitivity, and victim-centred approaches. The courts should be trained on various novel kinds of digital crimes and harms. The government should also design a standard operating procedures about how agencies should respond to cyber violence, in a time-sensitive manner. Workplaces and educational institutions should come up with systemic and sustainable measures that can assist electronic harassment victims. There should be clear reporting channels, accessible legal services, and other privacy-sensitive processes so that victims feel encouraged to report crimes.

The final component that our legal and policy framework requires is digital literacy. Individual awareness would empower people to identify and protest harassment, report cases earlier and access institutional resources. Use of social media platforms to improve reporting mechanisms should also be promoted and cooperation with national facilities should be mandated in effectively and promptly taking down online threats, doxing, or revenge porn.

Bangladesh is at a critical crossroads. The promises of justice and good governance will never be fulfilled unless online spaces are safe, gender-inclusive and rights-respecting. Sexual threats for exercising democratic agency must in no case be tolerated. Online harassment is not tantamount to mere online nuisance. It is an impediment to equality, democratic engagement, and fairness. To achieve this end, the law must be clear, proportionate and enforceable, supported by trained institutions, accessible reporting mechanisms and a gender-responsive public policy strategy. If Bangladesh is to promote democratic participation, safeguard freedom of expression and ensure that women can exist online without fear, its cyber governance must shift from reactive criminalisation to proactive protection. The challenge is substantial, but so is the necessity.

The writer is Associate Professor, Department of Law, University of Chittagong.

LAW VISION

The rise of tech-facilitated intimate partner violence in Bangladesh

ERA SHARMILA KHAN,
MD HASIB CHOWDHURY

Tech-facilitated intimate partner violence (TF-IPV) is the act of threatening, stalking or abusing a current or former partner through the misuse or abuse of technology. On the same note, technology-facilitated sexual violence (TFSV) involves a broad range of sexual abuse online, including sextortion, cyber harassment, sharing of images without consent and voyeurism, all of which are blatant abuses of privacy, consent, an array of individual rights and dignity.

In contrast to general cybercrimes, where the data or money is the target, TF-IPV attacks sexual autonomy and emotional well-being of the victims. The emergence of deepfakes, fake accounts and internet blackmail has moved traditional gender based violence into the virtual world. There is digital humiliation coupled with non-digital harm and damage to the victims. In Bangladesh, these abuses are not a far-off phenomenon anymore; they are occurring on a daily basis at the universities, offices, and within the four walls of households. It does not inflict physical bruises, but its psychological effect is severe.

A University student told the authors that "I blocked him on every social media platform, still he finds his way. I believe he is spying on me and it drives me insane". Such fear may lead to insomnia, panic attacks and social withdrawal. A sense of betrayal, which is caused by the emotional trauma of being abused by a loved one, intensifies the trauma, inculcating shame, guilt, and self-blame.

The new weapon in the digital arsenal is now Artificial Intelligence, which is now becoming a tool to harass, violate, defame, and shame women. Here, the catch is that many of the victims do not even consider taking any steps to vindicate their rights. This reflects their lack of confidence in the laws and their implementation process.

The Domestic Violence (Prevention and Protection) Act 2010 provides a definition of domestic violence as physical, sexual, economic, or emotional abuse, but fails to specifically mention digital violence. The Pornography Control Act 2012 criminalises non-consensual production and release of sexual images. The Cyber Safety Ordinance 2025 is yet another significant development in this context, as it categorically criminalises blackmailing, revenge pornography, sextortion and creation or distribution of AI-generated sexual materials. It also stipulates that severe punishments should be imposed in cases where women or minors are the victims. This is a major advancement as compared to the Cyber Security Act 2023 that emphasised mostly on hacking and financial fraud. Nevertheless, digital abuse cannot be solved only with help of legislation. It requires gender-sensitive investigations, trained officers, and procedures that focus on the survivors.

PHOTO: UN WOMEN

Tech facilitated intimate partner violence is not merely a cyber-crime, it is a psychological weapon undermining trust, safety and dignity. Justice is not just about prosecuting the abusers or erasing harmful material, but also about restoration of mental and emotional well-being of the survivor. Only with effective legal reform, survivor-based justice, and available mental health support, is it possible to ensure a safe cyber space for everyone.

In fact, Bangladesh needs to respond to TF-IPV and TFSV by initiating a multidimensional reform across legal, institutional, and mental health sectors. The Domestic Violence Act needs to be revised to accommodate digital gender-based violence. Much like any gender-based violence victims, cyber abuse victims are also victimised twice by the perpetrators and a conservative society that considers them as immoral or irresponsible or worse, responsible for the crimes. This victim-blaming culture increases the extent of trauma and discourages reporting. The victims also often have to face untrained police or insensitive court officials, which makes them relive the trauma.

A justice system that is informed by trauma and vulnerability is hence of utmost necessity. TF-IPV should be brought within the ambit of criminal laws and addressed effectively in order to close the legal, digital, and psychological gaps. Law enforcement officials, lawyers and judges are supposed to be trained to handle cases with increased sensitivity and empathy. The cybercrime departments ought to have counsellors or keep partnerships with mental health professionals. Women officers who are trained to deal with digital gender-based violence and referral systems across both legal aid and counselling services can help deliver justice and contribute to recovery of the victims. The Mental Health Act 2018 presents an option of community-based care, but it does not consider the trauma associated with digital abuse.

Moreover, digital consent, emotional abuse, and online ethics should be taught through public awareness activities, particularly in schools, colleges, universities, and in communities, targeting both women and men, to decrease the sense of stigma often associated with abuse. Sustained cooperation with technology platforms is also of paramount importance to delete objectionable content and tighten privacy policies. In the meantime, local mental health sites must improve access to community-based services that provide affordable mental health therapy, internet-based counselling and peer assistance. The ability to make survivors rebuild their self-esteem is equally essential as punishing the criminals. TF-IPV is not merely a cyber-crime, it is a psychological weapon undermining trust, safety and dignity. Justice is not just about prosecuting the abusers or erasing harmful material, but also about restoration of mental and emotional well-being of the survivor. Only with effective legal reform, survivor-based justice, and available mental health support, is it possible to ensure a safe cyber space for everyone.

The writers are apprentice lawyers of Dhaka Judge Court.