JNUS
JAGO NARI UNNAYON SANGSTHA

DISCUSSION PAPER
ON

TOWARDS DEVELOPING A GENDER-RESPONSIVE DIGITAL BANGLADESH: POLICY PATHWAYS TO PREVENT TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE

FEMINIST OPPORTUNITIES NOW

crea

AFD
AGENCE FRANÇAISE DE DÉVELOPPEMENT

DISCLAIMER:
THIS PUBLICATION WAS PRODUCED BY THE JAGO NARI UNNAYON SANGSTHA (JNUS), SUPPORTED BY FEMINIST OPPORTUNITIES NOW (FON) AND CREA. ITS CONTENTS ARE THE SOLE RESPONSIBILITY OF THE JNUS AND DO NOT NECESSARILY REFLECT THE VIEWS OF THE FON OR CREA.

Acknowledgements

This discussion paper summarizes the findings of desk research, fieldwork, and insights from the Young Women Leaders Forum (YWLF), a feminist network, civil society, media, women-led organizations, survivors and victims of TFGBV, and tech professionals, which focused on the trends in TFGBV in Bangladesh. JNUS conducted this study from April 2025 to January 2026, supported by Feminist Opportunities Now (FON) and CREA, USA. This discussion paper reflects the dedicated efforts of many individuals. Prepared by Mr. Ashish Banik, Lead Consultant at JNUS, the paper owes special thanks to Dr. Monira Ahshan, associated with JNUS as a research consultant, MR. Khandakar Zahid, former Programme Manager of JNUS and other members of the team for their immense contribution. Gratitude is also due to the members of YWLF who did the field work and extensively contributed to the development of this discussion paper. Finally, appreciation is extended to various stakeholders, including government officials, security service providers, representatives from INGOs and NGOs, local journalists, educators, community leaders, youth, security experts, and civil society members, for their valuable insights and assistance that shaped this paper.

Date of Publication
19 February 2026

Published by
Jago Nari Unnayon Sangstha (JNUS)
Ramu College Gate, Ramu Uapzilla
Cox's Bazar, Bangladesh
www.jagonariunnayon.org
+8801823929075, jagonariunnayon@gmail.com

Contents

Executive Summary 3

Introduction 7

1. Conceptual Framework: Understanding TFGBV in the Bangladesh Context 10

1.1 The Gender–Technology Nexus 10

1.2 Forms of Technology-Facilitated Gender-Based Violence 10

1.3 Intersectionality and Vulnerability 10

1.4 The Global and Regional Landscape 11

1.5 The Policy Imperative 11

2. Empirical Findings from the JNUS Field Study 12

2.1 Access to Digital Devices and Connectivity 12

2.2 Experiences and Patterns of TFGBV 13

2.3 Perception of Safety and Self-Censorship 13

2.4 Psychological, Social, and Economic Impacts 13

2.5 Reporting Behavior and Justice Pathways 14

2.6 Community Perceptions and Local Support Networks 14

2.7 Key Takeaways from Field Evidence 14

3. Data, Evidence, and Knowledge Gaps on TFGBV in Bangladesh 15

3.1 Structural and Methodological Gaps 16

3.2 Proposed Data and Evidence Architecture 16

3.3 Ethical Standards and Privacy Protection 17

3.4 Data and Artificial Intelligence for TFGBV Research 17

3.5 Recommendations for Data Strengthening 18

4. Strengthening Legal and Policy Frameworks 18

4.1 Current Legal Landscape 19

4.2 Policy and Legislative Reform Priorities 19
4.3 Strengthening Institutional Frameworks 19
4.4 Role of Regulatory Agencies and Oversight Bodies 20
5. Platform Accountability and Regulation 22
5.1 Role of Online Platforms in TFGBV 22
5.2 Principles for Platform Accountability 22
5.3 National Digital Safety and Accountability Charter 23
5.4 Algorithmic Transparency and Content Moderation 23
5.5 Addressing AI-Driven Harms 23
5.6 Regional and Global Cooperation 24
6. Prevention through Education and Capacity Building 25
6.1 Building Digital Literacy and Responsible Online Behavior 25
6.2 Strengthening Law Enforcement and Judicial Capacity 25
6.3 Mental Health and Psychosocial Support 26
6.4 Civil Society and Private Sector Engagement 26
6.5 Promoting Digital Safety Leadership and Youth Engagement 26
6.6 Institutionalizing Prevention in National Policy Frameworks 27
7. Strategic Framework for Implementation 28
7.1 Multi-Stakeholder Coordination Mechanism 28
7.2 Financing and Resource Mobilization 28
7.3 Monitoring, Evaluation, and Learning (MEL) 29
7.4 Communication and Advocacy Strategy 29
Conclusion 30

Executive Summary

In alignment with the 2025 theme for the 16 Days of Activism against Gender-Based Violence, **"UNiTE to End Digital Violence against All Women and Girls,"** this publication serves to commemorate the global campaign while guiding government and non-government stakeholders in Bangladesh to strengthen their efforts against Technology-Facilitated Gender-Based Violence (TFGBV). The rapid expansion of the digital landscape in Bangladesh has brought about complex challenges, primarily driven by uneven digital literacy, a widening digital divide, and a persistent gender gap. TFGBV, therefore, has rapidly emerged as a critical challenge to digital safety, human rights, and gender justice in Bangladesh, necessitating urgent and coordinated prevention efforts. Consequently, the promise of digital inclusion is increasingly undermined by pervasive forms of online abuse, including cyberstalking, non-consensual image sharing, revenge pornography, sextortion, deepfakes, growing digital divide, unequal access to digital devices and algorithmically amplified gendered harassment.[1] While TFGBV disproportionately affects women and girls, it also specifically targets gender diverse population, human rights defenders, journalists, and other socially marginalized groups whose intersecting vulnerabilities exacerbate their exposure to digital harm. Ultimately, such abuse does more than violate personal safety and dignity—it effectively silences voices, restricts participation in public life, and undermines the core of democratic engagement.[2]

Recent national reporting indicates that over 78% of women in Bangladesh have experienced some form of technology-based violence, with social media platforms such as Facebook and messaging applications frequently cited as the primary sites of abuse. This digital violence is deeply tied to adverse psychosocial outcomes, as the trauma of online harassment often extends far beyond the digital realm. Consequently, a significant proportion of survivors report severe mental health impacts, including anxiety, depression, and social withdrawal.[3] Moreover, underreporting remains a major barrier to redress: only a small fraction of victims pursue formal complaints due to stigma, low trust in legal systems, and lack of awareness about reporting mechanisms.

To address the emerging threat of digital violence, including Technology-Facilitated Gender-Based Violence (TFGBV), the Government of Bangladesh has undertaken various institutional

---

[1] UN Women. (2023). *Gendered disinformation and technology-facilitated gender-based violence: Global guidance for policymakers.* https://www.unwomen.org/en/digital-library/publications/2023/09/gendered-disinformation-and-technology-facilitated-gender-based-violence & United Nations. (2024). *Global Digital Compact*. https://www.un.org/global-digital-compact

[2] United Nations Bangladesh. (2023). *Bangladesh hosts national dialogue to end digital violence as part of global 16 Days of Activism.*

[3] The Daily Star. (2024, January 28). *Over 78% women face tech-based violence in Bangladesh*. https://www.thedailystar.net/news/bangladesh/news/over-78pc-women-face-tech-based-violence-bangladesh-3774116

and legal measures. While the state has prioritized cybercrime enforcement by establishing dedicated support units and enhancing the institutional capacity of law enforcement, significant gaps remain within the statutory framework. Historically, the Digital Security Act (DSA) 2018 and its successor, the Cyber Security Act (CSA) 2023, were criticized for focusing more on speech regulation than on providing comprehensive protections for victims of digital abuse. In a major reform move, the interim government repealed the CSA and issued the Cyber Security Ordinance (CSO) 2025 on May 21, 2025. Although this new ordinance introduces the landmark recognition of internet access as a civic right and specifically identifies AI-facilitated crimes and the sexual harassment of women and children in cyberspace as punishable offenses, legal experts argue that existing frameworks, including the Pornography Control Act (2012), still lack the precise definitions needed to fully criminalize complex modern threats like gendered disinformation and algorithmically enabled harassment.[4] This legislative gap undermines effective prosecution and accountability and contributes to persistent impunity.

Prepared by **Jago Nari Unnayan Sangstha (JNUS)** with support from Feminist Opportunity Now (FON) and CREA, this discussion paper aims to present evidence-informed and actionable policy pathways to prevent and respond to Technology-Facilitated Gender-Based Violence (TFGBV) in Bangladesh. The recommendations contained herein are specifically designed for the Government of Bangladesh, policymakers, civil society, and development partners. The strategy proposed in this document is built upon a dual foundation: it draws on international frameworks and global norms, including CEDAW, the Beijing Platform for Action, the Global Digital Compact (2024), and the OECD's 2024 Digital Safety Principles, while simultaneously grounding these standards in local realities. Specifically, it builds on the findings of the **Young** Women Leaders Forum (YWLF), a feminist network that facilitated extensive dialogues and focus group discussions across urban, semi-urban, and rural areas of Bangladesh. By synthesizing global standards with these grassroots insights, this paper proposes a comprehensive, multi-stakeholder strategy for a safer digital future for Bangladesh.

Policy Recommendations

1. Strengthening Governance and Institutional Coordination: Effective prevention and response to any form of digital violence including TFGBV would require strong institutional leadership and coordinated governance mechanisms. It is recommended that the Government of Bangladesh should establish an inter-ministerial National Task Force to address this emerging but challenging issues, bringing together the Ministry of Women and Children Affairs (MoWCA), the Ministry of Information and Communication Technology (MoICT), the Bangladesh Telecommunication Regulatory Commission (BTRC), law enforcement agencies, and relevant civil society organizations. This Task Force could serve as a central coordination body to harmonize policy actions, align mandates, and ensure

[4] Bangladesh Legal Aid and Services Trust (BLAST). (2021). *Cyber violence against women in Bangladesh: Legal gaps and challenges*.
https://www.blast.org.bd/content/publications/Cyber-violence.pdf

accountability across sectors. In addition, the creation of dedicated TFGBV focal points at district and upazila levels might strengthen decentralized response mechanisms by enabling rapid case referral, survivor support, and systematic data reporting, thereby bridging national policy with local implementation.

2. Legal and Policy Reform: Bangladesh's existing legal frameworks require urgent reform to address the evolving nature of digital violence including TFGBV. National cyber and criminal laws should be amended to explicitly define and criminalize TFGBV-related offences, including deepfake pornography, doxxing, cyberstalking, online impersonation, harassment and gendered disinformation. Legal reform must also ensure survivor-centered justice, including robust protections for victim privacy, expedited judicial processes, and the formal inclusion of TFGBV-related evidence within the Evidence Act. Given the transnational character of digital platforms and online crimes, Bangladesh should further pursue regional and global cooperation mechanisms, particularly through regional and global frameworks, to enhance cross-border investigation, information sharing, and mutual legal assistance in cases of TFGBV.

3. Partnership with Online Platforms and the Private Sector: Addressing TFGBV effectively necessitates meaningful engagement with online platforms and private sector actors that shape digital ecosystems. Government regulatory authorities must oblige social media companies to publish regular transparency reports detailing content moderation practices, response timelines, and the prevalence of gender-based harassment on their platforms. Furthermore, major technology platforms, including Meta, TikTok, and YouTube, should be mandated to maintain local liaison offices or designated representatives to facilitate coordination with national regulators, law enforcement agencies, and civil society organizations. A co-regulatory model is also recommended, whereby civil society actors can actively monitor and assess platform compliance with national digital safety guidelines, thereby reinforcing accountability while preserving freedom of expression and core principles of Human Rights.

4. Prevention through Education and Awareness: Long-term prevention of TFGBV depends on embedding digital literacy, safety, ethics, reducing digital divide, strengthening equal access to digital tools and gender equality within educational and social systems. Digital citizenship, cyber ethics, and gender-responsive online safety should be systematically integrated into the National Curriculum Framework at secondary and tertiary levels. Complementing formal education, a nationwide "Safe Digital Bangladesh" campaign should be launched to engage youth, journalists, content creators, and social media influencers in promoting responsible online behavior and countering harmful narratives. At the community level, government institutions, particularly MoWCA, should partner with local NGOs to support community-based digital safety champions, with a particular emphasis on strengthening the leadership of young women as advocates for safer digital spaces.

5. Data, Research, and Evidence Generation: Robust data and continuous research are critical to evidence-informed policymaking on TFGBV. It is recommended that TFGBV-specific data modules be institutionalized within national data collection instruments, including the Bangladesh Bureau of Statistics' (BBS) Violence Against Women surveys and Demographic and Health Surveys. Strategic partnerships with universities and research institutions should be established to develop national TFGBV dashboards that track prevalence, patterns, institutional responses, and policy gaps over time. Additionally, public–private research collaborations with telecommunications providers and AI companies should be encouraged to enable anonymized data analysis, guided by strong ethical safeguards and data protection standards, to better understand digital violence trends without compromising individual privacy.

6. AI Governance and Emerging Threats: The rapid advancement of artificial intelligence and generative technologies presents new and complex risks for TFGBV, including deepfake abuse and automated harassment. Bangladesh should invest in AI misuse detection systems and establish national reporting databases for deepfakes and synthetic media crimes. In parallel, the development of ethical standards for AI developers and digital platforms is essential. These standards should be aligned with international benchmarks, including the OECD AI Principles and the EU Artificial Intelligence Act (2024), to address algorithmic bias, ensure transparency, and establish clear accountability mechanisms for AI-enabled harms.

7. Monitoring, Evaluation, and Accountability: To ensure sustained progress and transparency, a strong monitoring and accountability framework must underpin all TFGBV interventions. The introduction of a National TFGBV Index under a broader framework of digital violence is recommended to systematically track progress across key dimensions, including data availability, legal reform, enforcement capacity, survivor support services, and public awareness. Annual multi-stakeholder review processes, led by MoWCA or any other relevant government bodies with active participation from civil society organizations, women-led organizations in particular and academic institutions, should be institutionalized to assess implementation outcomes and identify emerging gaps. Finally, the regular and transparent publication of TFGBV case data, service provision statistics, and policy outcomes will be essential to strengthen public trust, inform advocacy, and uphold state accountability.

Collectively, these recommendations have been envisioned to promote a gender-responsive, rights-based, and resilient digital ecosystem in Bangladesh, where technology could serve as an enabler of opportunity and empowerment rather than a conduit for violence and exclusion. Integrating legal reform, institutional coordination, prevention through education, and ethical technology governance will not only reduce TFGBV but also strengthen women's equitable participation in the digital society

Introduction

TFGBV refers to acts of abuse, harassment, exploitation, and harm that are perpetrated, enabled, or amplified through digital technologies and online platforms. It encompasses a wide spectrum of behaviors, including cyberstalking, online harassment, doxxing, impersonation, non-consensual image and video sharing, gendered disinformation, sextortion, and the production and circulation of deepfake pornography. Increasingly, TFGBV is facilitated by algorithmic systems, artificial intelligence (AI), and data-driven infrastructures that can intensify the scale, speed, and persistence of harm.[5] Importantly, technology-facilitated violence does not happen in isolation from the real world. Instead, it moves fluidly between online and offline spaces, reinforcing existing social inequalities such as gender, disability, and class.[6]

Bangladesh's rapid digital transformation, driven by various national commitments, has significantly expanded access to information, education, financial services, and civic participation. As of the end of 2025, Bangladesh had approximately 131.5 million internet subscribers, the vast majority of whom accessed the internet through mobile connections, highlighting the country's expanding digital reach and the significant role of online platforms in communication, social interaction, and economic activity.[7] However, this expansion has also heightened exposure to digital risks, particularly for women, girls, and gender-diverse people. National studies indicate that a majority of women internet users in Bangladesh have experienced some form of technology-based abuse, with online harassment and non-consensual image sharing among the most prevalent forms.[8]

The impacts of TFGBV in Bangladesh are both pervasive and multidimensional. Survivors frequently report psychological distress, including anxiety, depression, fear, and social withdrawal, alongside reputational damage and threats to physical safety. These harms translate into broader socio-economic consequences, such as educational dropout, reduced workforce participation, loss of income, and self-censorship in public and digital spaces.[9] Technology-

---

[5] Organisation for Economic Co-operation and Development. (2024). *OECD principles on digital security risk management and gender equality*. https://www.oecd.org/digital/security & UN Women. (2023). *Gendered disinformation and technology-facilitated gender-based violence: Global guidance for policymakers*. https://www.unwomen.org/en/digital-library/publications/2023/09/gendered-disinformation-and-technology-facilitated-gender-based-violence

[6] CEDAW Committee. (2017). *General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19* (CEDAW/C/GC/35). United Nations Office of the High Commissioner for Human Rights. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-35-gender

[7] Bangladesh Telecommunication Regulatory Commission. (2025). *Internet subscriber statistics – 2025*. Retrieved from https://btrc.gov.bd/site/page/347df7fe-409f-451e-a415-65b109a207f5/ (Accessed 2025).

[8] The Daily Star. (2024, January 28). *Over 78% women face tech-based violence in Bangladesh.* https://www.thedailystar.net/news/bangladesh/news/over-78pc-women-face-tech-based-violence-bangladesh-3774116

[9] Jago Nari Unnayan Sangstha. (2025). *Focus group discussions with members of the Young Women Leaders Forum (YWLF) in Chattogram, Cox's Bazar, and Rangpur (June–July 2025)*

Facilitated Gender-Based Violence (TFGBV) often functions as a deliberate mechanism of silencing, directly curtailing freedom of expression and limiting participation in democratic processes. This impact is especially profound for journalists, human rights defenders, and young women leaders who rely on digital spaces for advocacy and professional engagement. Furthermore, intersectional vulnerabilities—including poverty, rural isolation, and limited digital literacy—combined with entrenched gender norms, exacerbate exposure to abuse while simultaneously restricting access to justice for marginalized groups.[10]

Significant gaps remain in Bangladesh's institutional and legal responses, which hinder the state's ability to effectively address emerging trends such as deepfakes, gendered disinformation, and AI-enabled harassment. Furthermore, there are limitations and challenges in current frameworks to adequately ensure survivor-centered protection or provide accessible pathways for legal redress. Additionally, effective prevention and response efforts are significantly constrained by gaps in data collection and limited coordination among state institutions. These challenges are further compounded by a lack of sufficient accountability mechanisms to hold online platforms responsible for the content they host. Despite these drawbacks, addressing TFGBV is not peripheral but central to Bangladesh's commitments to gender equality, human rights, and inclusive digital development. International normative frameworks, including the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the Beijing Platform for Action, the Global Digital Compact (2024), and the OECD's Digital Safety and AI governance principles, underscore state obligations to prevent digital harms, regulate corporate actors, and ensure safe, equitable participation in digital life (CEDAW Committee, 2017; United Nations, 2024; OECD, 2024). Aligning national policy with these frameworks is essential to ensuring that technological advancement in Bangladesh serves as a force for empowerment rather than exclusion.

This discussion paper is organized into seven sections. The first section establishes the conceptual frameworks relating to TFGBV, while the second section documents women's lived experiences of digital harassment, surveillance, and reputational abuse, highlighting their severe psychological, social, and economic impacts. Moving toward systemic solutions, the third section identifies critical gaps in national data systems and institutional coordination, proposing ethical, survivor-centered evidence architecture for informed policymaking. The fourth section examines Bangladesh's existing legal and policy landscape, outlining priorities for legal reform, institutional capacity building, and cross-border cooperation to overcome current enforcement challenges. Addressing the technological drivers of abuse, the fifth section analyzes the role of digital platforms and AI systems, advocating for robust regulatory frameworks and accountability standards. The sixth section advances a prevention-centered approach through digital literacy, youth leadership, and community engagement to strengthen digital resilience and

[10] Plan International. (2020). *Free to be online? Girls' experiences of online harassment*. https://plan-international.org/publications/free-be-online/

challenge harmful norms. Finally, the seventh section presents a multisectoral implementation strategy, integrating governance coordination, sustainable financing, and advocacy to operationalize a holistic, rights-based, and feminist response to TFGBV in Bangladesh.

Members of YWLF are delivering the findings of FGD

1. Conceptual Framework: Understanding TFGBV in the Bangladesh Context

1.1 The Gender–Technology Nexus

Digital technologies are not neutral or uniformly empowering. Instead, they are intricately intertwined with existing social, cultural, and political power dynamics. The interplay of patriarchal norms, unequal access to digital resources, pronounced polarization across communities and institutions, and expanding digital divide in Bangladesh has created a profoundly gendered digital ecosystem. While digital platforms offer new opportunities for communication, learning, and participation, they simultaneously reproduce and intensify gender-based control and violence. Women's access to technology in Bangladesh is often mediated by family approval, economic dependency, harmful gender norms, and moral scrutiny. Restrictions on device ownership, monitoring of online activities by family members, and social expectations around "appropriate" digital behavior often expose women and girls to both exclusion and punishment. Limited digital literacy, coupled with entrenched victim-blaming attitudes, further constrains women's ability to navigate online risks and seek redress. Within this context, gender hierarchies are enforced, and technology is frequently used as a tool to police, intimidate, and silence women in rural and semi-urban areas compared to urban settings.

1.2 Forms of Technology-Facilitated Gender-Based Violence

TRGBV in Bangladesh manifests in multiple, often overlapping forms. Cyber harassment and stalking involve persistent, unwanted digital contact, monitoring, or threats that generate fear and psychological distress. Image-based abuse, including the non-consensual creation, manipulation, or circulation of intimate images and videos, increasingly through AI-generated deepfakes, has become one of the most devastating forms of TFGBV, with severe reputational and social consequences for survivors. Gendered disinformation represents a growing threat in Bangladesh's digital public sphere, where coordinated online campaigns are used to undermine women's credibility, leadership, or moral standing, particularly those engaged in activism, journalism, or politics. Online hate speech, rooted in misogyny reinforces exclusion and legitimizes violence against women and gender-diverse individuals. The unauthorized disclosure of personal information, commonly referred to as doxxing and data misuse, exacerbates safety concerns by subjecting survivors to offline harassment and potential physical harm. These forms of abuse rarely occur in isolation. Rather, they exist along a continuum of violence, where digital aggression frequently escalates into offline intimidation, social exclusion, economic harm, or physical violence, blurring the boundaries between virtual and physical spaces.

1.3 Intersectionality and Vulnerability

Exposure to TFGBV in Bangladesh is shaped by intersecting axes of identity and power. Young women, gender diverse individuals, journalists, activists, and public figures face heightened risks due to their visibility, advocacy roles, or challenges to dominant social norms. For many

survivors, digital violence is compounded by structural inequalities related to class, geography, disability, identity crisis and access to education, particularly in rural and marginalized communities. If statements of gender diverse populations are to be believed, a defining feature of TFGBV in Bangladesh is secondary victimization. Survivors frequently encounter social stigma, moral judgment, and institutional indifference after they report abuse. Fear of reputational damage, family retaliation, or professional consequences mostly discourages disclosure and reporting, reinforcing the cycles of silence and impunity. These dynamics highlight that vulnerability to TFGBV is not merely individual but is structurally produced through social norms, institutional gaps, and unequal power relations.

1.4 The Global and Regional Landscape

International normative frameworks, such as CEDAW General Recommendation No. 35, the Beijing Platform for Action, and the Global Digital Compact (2024), affirm the obligation of states to prevent gender-based violence in digital spaces and ensure safe, inclusive, and rights-based access to technology. These frameworks increasingly recognize TFGBV as a human rights violation, necessitating regulatory oversight, corporate accountability, and survivor-centered remedies. At the regional level, initiatives within regional and sub-regional bodies indicate a growing recognition of the cross-border nature of digital violence and the need for coordinated responses to cybercrimes and online gender-based abuse. For Bangladesh, meaningful engagement with regional and global processes is essential to harmonize legal standards, strengthen cross-border cooperation, and address the transnational dimensions of TFGBV facilitated by global and regional platforms.

1.5 The Policy Imperative

Addressing TFGBV in Bangladesh would require a comprehensive and transformative policy approach that transcends mere technological regulation. While legal reform and institutional coordination are essential, they must be augmented by multi-stakeholder efforts to challenge the socio-cultural norms that perpetuate harassment, silence survivors, and legitimize digital control over women's lives. Therefore, effective national strategies should incorporate feminist digital justice principles, ensuring survivor-centered processes, ethical governance of emerging technologies such as artificial intelligence, and equitable access to digital participation. This policy imperative should also highlight that structural problems rooted in gender inequality, power dynamics and accountability crisis need to be dealt following a whole of society approach.

2. Empirical Findings from the JNUS Field Study

Between September 2024 and August 2025, JNUS conducted a qualitative field study to investigate the lived experiences, perceptions, and responses to TFGBV among young women and community members in Bangladesh. Supported by Feminist Opportunity Now (FON) and CREA, the study engaged 162 participants, comprising 132 women and girls and 30 men, aged 16 to 35, across three divisions and one district: Barishal, Rangpur, Chattogram, and Cox's Bazar, encompassing rural, semi-urban, and urban areas. Conducting Focus Group Discussions (FGDs) and key Informant Interviews (KII), the research examined how digital spaces had been navigated, how risks manifested, and how structural, social, and institutional barriers influenced prevention, reporting, and justice-seeking. The findings elucidated the interconnections between trends in TFGBV, the digital divide and access, gender norms, and governance gaps within Bangladesh's evolving digital ecosystem.

2.1 Access to Digital Devices and Connectivity

Despite expanding national connectivity, the study reveals a persistent and deeply gendered digital divide. While most male participants reported owning personal smartphones, fewer than 40 percent of women indicated ownership of a private device, with many relying on shared or family-owned phones. This dependence significantly limited their privacy, autonomy, and control over digital engagement. Participants from rural areas, particularly in Cox's Bazar, highlighted compounded constraints arising from poverty, restrictive gender norms, and cultural expectations that discourage women's independent use of technology. Across sites, women reported limited awareness of privacy controls, account recovery mechanisms, and basic cybersecurity practices, increasing their exposure to digital surveillance, impersonation, and abuse. These conditions reinforce women's dependence on male guardians, normalize monitoring of women's online activities, and undermine the transformative potential of digital access.

2.2 Experiences and Patterns of TFGBV

Across all locations, participants consistently identified social media platforms, especially Facebook, TikTok, and Whats'app, as primary sites of technology-facilitated abuse. Common experiences reported by participants included persistent cyber harassment through unsolicited sexualized messages and comments across social media platforms. Many also faced impersonation and the creation of fake accounts using manipulated or stolen images, as well as non-consensual sharing of images and videos, often linked to blackmail or extortion. In addition, gendered disinformation was widespread, with rumors and moral accusations deliberately circulated online to undermine women's credibility and damage their personal and professional reputations. These forms of abuse were rarely isolated incidents, instead unfolding as sustained campaigns of intimidation. One participant from Chattogram described how posting lifestyle content triggered anonymous harassment, followed by the creation of fake profiles using her images and threats of public exposure. The cumulative psychological harm ultimately led her to discontinue her education, a trajectory echoed by multiple participants, highlighting how online abuse escalates into profound social, emotional, and economic consequences.

2.3 Perception of Safety and Self-Censorship

A pervasive sense of insecurity shaped women's digital participation across study sites. Approximately three out of four women reported practicing self-censorship, deliberately avoiding personal photographs, opinions, or public engagement online due to fear of harassment, misinterpretation, or moral judgment. Cultural and religious norms further intensified these fears, particularly in rural contexts where community surveillance and victim-blaming are deeply entrenched. Participants noted that families frequently responded to incidents of online harassment by restricting women's device use, mobility, or digital expression rather than holding perpetrators accountable. Such responses reinforce patriarchal control, shift responsibility onto survivors, and contribute to women's withdrawal from digital spaces.

2.4 Psychological, Social, and Economic Impacts

The impacts of TFGBV documented in the study were multidimensional and long-lasting. Participants reported significant psychological distress, including anxiety, depression, insomnia, and diminished self-worth. Educational disruption emerged as a common consequence, with several women discontinuing school or higher education due to fear, stigma, or reputational damage. Social isolation and community ostracization were frequently cited, particularly where abuse was publicly visible. Economic repercussions included job loss, withdrawal from income-generating activities, or reduced employment opportunities linked to perceived moral transgression. In several cases, online threats escalated into offline stalking or physical intimidation, underscoring the blurred boundary between digital and physical violence.

Collectively, these harms erode women's digital citizenship and constrain their participation in economic, social, and civic life.

2.5 Reporting Behavior and Justice Pathways

Despite recognizing TFGBV as harmful and unjust, the majority of participants had not reported incidents to formal authorities. Reporting was inhibited by fear of social stigma, retaliation, and reputational damage, alongside widespread distrust in police responsiveness and judicial processes. Limited awareness of legal protections under the Digital Security Act (2018) further constrained help-seeking. Many participants perceived online harassment as insufficiently serious to warrant legal action or believed that reporting would exacerbate harm rather than provide protection. Initial disclosures were typically made to friends or family members. However, familial interventions often prioritized social control over justice, resulting in restrictions on internet use or behavioral monitoring rather than engagement with legal remedies.

2.6 Community Perceptions and Local Support Networks

At the community level, awareness of TFGBV and capacity to respond effectively remain limited. Even among educated youth, understanding of digital consent, privacy rights, and ethical online behavior was inconsistent. While local NGOs, youth groups, and informal networks occasionally provided support, interventions were largely ad hoc and lacked coordination or sustainability. Participants emphasized the absence of safe, stigma-free spaces where survivors could share experiences and seek guidance. The findings highlight a strong demand for community-based digital literacy initiatives, peer mentorship, and locally grounded support mechanisms that are sensitive to gender, age, and socio-cultural context.

2.7 Key Takeaways from Field Evidence

The field evidence underscores several critical insights. First, TFGBV is widespread yet profoundly underreported, with silence often adopted as a survival strategy. Second, gaps in digital literacy and privacy awareness significantly heighten vulnerability to abuse and surveillance. Third, institutional mistrust and limited legal awareness discourage formal reporting and redress. Fourth, the consequences of TFGBV, particularly psychosocial distress and educational disruption, are long-term and deeply gendered. Finally, participants consistently identified **community-driven prevention mechanisms**, including awareness-building, peer support, and youth leadership, as essential to strengthening local resilience against digital violence. Effective policy responses to TFGBV require robust, timely, and disaggregated data. Yet, in Bangladesh, information on TFGBV remains fragmented, anecdotal, and heavily underreported. Without comprehensive data, the true scale, patterns, and consequences of online gender-based violence remain obscured, hindering the design of evidence-informed interventions.

3. Data, Evidence, and Knowledge Gaps on TFGBV in Bangladesh

Bangladesh currently lacks a centralized, systematic mechanism to document and analyze digital violence. Existing data are fragmented across multiple entities, including the Digital Security Agency, the Bangladesh Police Cyber Crime Unit, and civil society organizations. These datasets are typically limited in scope, inconsistently recorded, and largely uncoordinated. Most incidents are categorized under broad headings such as cybercrime, defamation, or fraud, without gender-specific classification or analysis. As a result, TFGBV remains statistically invisible within formal governance systems. Compounding this challenge, the Bangladesh Bureau of Statistics (BBS) does not currently incorporate TFGBV-specific indicators within national gender, violence, or ICT-related surveys, constraining the ability of policymakers to identify trends, risk factors, and structural patterns over time.

3.1 Structural and Methodological Gaps

Several interrelated structural and methodological gaps undermine the production of reliable TFGBV data in Bangladesh. First, systemic underreporting persists due to social stigma, victim-blaming, fear of retaliation, and concerns about reputational harm. Many survivors opt for informal resolution within families or communities, preventing cases from entering official reporting systems. Second, the absence of standardized national definitions of TFGBV leads to inconsistent categorization across institutions, obscuring comparability and aggregation of data. Third, the lack of disaggregated data, by gender, age, geography, disability, or sexual identity, limits the ability to assess intersectional vulnerabilities. Fourth, institutional capacity constraints remain significant, as law enforcement officials and data officers often lack specialized training to identify, classify, and document TFGBV sensitively and accurately. Finally, restricted access to platform-generated data poses a critical limitation, as social media and technology companies retain extensive information on harassment dynamics that remains largely inaccessible to regulators, researchers, and policymakers in Bangladesh.

3.2 Proposed Data and Evidence Architecture

To address these systemic gaps, this paper proposes the establishment of a National TFGBV Data and Research Framework designed to support evidence-informed policymaking and prevention-oriented governance. This framework should emphasize institutional coordination, standardized methodologies, and ethical data management. Central to this architecture is the integration of state agencies, statistical institutions, academic bodies, civil society organizations, and private sector actors into a coherent national ecosystem for TFGBV data generation, analysis, and dissemination. At the core of the proposed framework, a National TFGBV Observatory might be established under the Ministry of Women and Children Affairs (MoWCA) or any specialized body of the government. The Observatory could function as a multi-sectoral coordination and analytical hub, responsible for consolidating data from BBS, BTRC, the Digital Security Agency, law enforcement agencies, academic institutions, and civil society organizations. Through standardized indicators and shared reporting protocols, the Observatory could enable systematic tracking of TFGBV prevalence, patterns, geographic distribution, and legal outcomes. A publicly accessible national dashboard could further enhance transparency, support research, and inform policy interventions while maintaining survivor confidentiality.

- **Integration into National Surveys:** Mainstreaming TFGBV within national data systems is essential for generating longitudinal and population-level evidence. This paper recommends integrating TFGBV-specific modules into existing instruments such as the Demographic and Health Surveys (DHS), Violence Against Women (VAW) surveys, and ICT Access and Use surveys. These modules should collect gender and age-disaggregated data

on device ownership, online experiences, safety perceptions, and exposure to digital harm. In addition, periodic youth-focused digital safety surveys should be conducted to capture emerging risks affecting adolescents and students, whose online engagement is expanding rapidly and whose vulnerabilities are often underrepresented in national datasets.

- **Data Partnerships with Tech Platforms:** Given the central role of digital platforms in shaping online interactions, structured data partnerships with technology companies are critical. The Government of Bangladesh should pursue formal data-sharing agreements with major social media and telecommunications providers to access anonymized and aggregated datasets on harassment patterns, reporting behavior, and response timelines. Platforms should also be required to publish regular transparency reports that include gender-disaggregated data on content removals, user complaints, and enforcement actions. The responsible use of AI-enabled monitoring tools can further support the detection of trends in online hate speech, coordinated harassment, and gendered misinformation, provided such tools operate within robust ethical and legal safeguards.

3.3 Ethical Standards and Privacy Protection

All TFGBV data collection and analysis must adhere to stringent ethical standards grounded in survivor safety, confidentiality, and the principle of "do no harm." Ethical governance may consider adopting UN Women's (2023) guidelines on ethical data collection for gender-based violence, including informed consent, voluntary participation, and trauma-sensitive methodologies. All personally identifiable information must be anonymized prior to analysis or dissemination, and access to sensitive datasets should be strictly controlled. Data protection protocols should be aligned with international best practices to prevent misuse, re-identification, or secondary harm.

3.4 Data and Artificial Intelligence for TFGBV Research

The strategic use of data and artificial intelligence presents significant opportunities to enhance understanding of TFGBV in real time. AI-enabled text analytics and pattern recognition tools can assist policymakers and researchers in identifying spikes in online hate speech, mapping geographic clusters of cyberstalking or harassment, and tracking misinformation narratives targeting women in public life. However, the deployment of such technologies must be transparent, rights-based, and subject to independent oversight. Partnerships with academic institutions and ethical AI research centers can help ensure methodological rigor, mitigate algorithmic bias, and establish accountability mechanisms while leveraging technological innovation for public good.

3.5 Recommendations for Data Strengthening

To institutionalize a sustainable and rights-based TFGBV data ecosystem, this paper recommends the development of a national TFGBV data protocol with unified definitions, indicators, and reporting templates applicable across institutions. A centralized online reporting platform should be established to allow survivors and witnesses to report TFGBV safely and anonymously. Continuous capacity building for law enforcement, statisticians, researchers, and frontline responders is essential to strengthen gender-sensitive data collection and analysis. Annual data publications on digital violence should be introduced to enhance transparency, inform policy adjustments, and enable public accountability. Finally, Bangladesh should engage with regional frameworks and other relevant global platforms to support comparative research and cross-border policy learning. Reliable, disaggregated, and ethically managed data are essential to shifting policy responses from reactive case management toward proactive, prevention-oriented, and rights-based digital governance. By investing in coordinated data systems, ethical innovation, and institutional capacity, Bangladesh can lay the foundation for safer, more inclusive digital environments that uphold dignity, accountability, and gender justice.

Ms. Sheuly Sharma, Executive Director of JNUS, is addressing a National Advocacy Dialogue in Dhaka

4. Strengthening Legal and Policy Frameworks

A robust and coherent legal and policy framework is fundamental to the prevention, investigation, and prosecution of TFGBV. While Bangladesh has demonstrated commitment to addressing cybercrime and gender-based violence through various legislative instruments, the existing framework remains fragmented and insufficiently responsive to rapidly evolving digital harms. Strengthening legal and policy responses to TFGBV therefore requires not only targeted legal reform but also institutional alignment to ensure effective enforcement, survivor-centered justice, and accountability of technology actors operating within the country's digital ecosystem.

4.1 Current Legal Landscape

While Bangladesh's legal architecture addresses certain dimensions of online violence, the current framework remains fragmented and fails to comprehensively regulate the full spectrum of TFGBV. Historically, the Digital Security Act (DSA) 2018 focused heavily on cybercrime and defamation but lacked the gender-sensitive clarity needed to address non-consensual digital acts. Its successor, the Cyber Security Act (CSA) 2023, attempted to modify some punitive measures but largely retained the structural limitations of the previous regime. Most recently, the Cyber Security Ordinance (CSO) 2025 has been introduced by the interim government to align digital governance with human rights and recognize AI-facilitated crimes. However, it is still being integrated into a landscape where the Pornography Control Act (2012) fails to adequately cover synthetic deepfakes, and the ICT Act (2006) remains outdated against modern generative technologies. Furthermore, while the Evidence Act (Amendment 2023) now recognizes digital data, it lacks the specific gender-responsive guidelines found in the Nari o Shishu Nirjatan Daman Ain (2000), which itself continues to exclude technology-mediated offenses. Collectively, the transition from the DSA and CSA to the 2025 Ordinance reflects progress, yet the ongoing absence of unified definitions and gender-responsive interpretation creates legal loopholes that continue to enable impunity for perpetrators.

4.2 Policy and Legislative Reform Priorities

Strengthening Bangladesh's legal response to TFGBV requires a comprehensive and coordinated reform agenda. A critical step in addressing TFGBV is its formal legal recognition as a distinct form of gender-based violence through a dedicated legal framework. Such a framework should clearly define and criminalize emerging forms of online abuse, including deepfake exploitation, gendered disinformation, impersonation, and AI-enabled harassment. It should also provide for aggravated penalties in cases involving repeat offenders or coordinated online hate campaigns to ensure effective deterrence and accountability. Equally critical is the harmonization of TFGBV-related definitions and provisions across existing statutes, such as the Digital Security Act, Penal Code, ICT policies, and evidence laws, to eliminate inconsistencies and strengthen enforcement, alongside the integration of gender-sensitive protections within data protection and privacy legislation and the formal inclusion of TFGBV in the National Action Plan on Violence against Women.

4.3 Strengthening Institutional Frameworks

Legal reform must be complemented by institutional capacity building to translate law into practice. Law enforcement agencies should establish dedicated TFGBV units within cybercrime divisions, staffed by trained personnel, including female officers, and supported by specialized digital forensic expertise. Judicial actors require continuous capacity development through training modules on TFGBV evidence, survivor protection, and digital ethics to ensure fair and

informed adjudication. Survivor-centered justice must be reinforced through confidential reporting mechanisms, trauma-informed procedures, and gender-responsive witness protection. In parallel, access to free legal aid and counseling should be expanded to reduce barriers to justice.

4.4 Role of Regulatory Agencies and Oversight Bodies

Effective governance of TFGBV requires clearly defined mandates, strong institutional coordination, and accountability across regulatory, security, and rights-based bodies. The Bangladesh Telecommunication Regulatory Commission (BTRC) should play a proactive regulatory role by monitoring digital platforms and telecommunications operators for compliance with national digital safety and content governance standards. The Ministry of Information and Communication Technology (MoICT) is well positioned to lead policy harmonization and coordinate national digital safety strategies across sectors, including alignment with data protection, cyber security, and emerging technology governance frameworks. The Ministry of Women and Children Affairs (MoWCA) should serve as the lead agency for survivor-centered prevention, protection, and inter-agency coordination on TFGBV, ensuring that gender and rights considerations remain central to all digital safety initiatives. The National Telecommunication Monitoring Center (NTMC) can contribute technical intelligence and threat analysis related to digital misuse and coordinated online harassment, while operating within strict legal and human rights safeguards. The Cyber Crime Unit of the Bangladesh Police can play a critical enforcement role through investigation, digital forensics, and prosecution of TFGBV-related offences, necessitating specialized training and gender-sensitive procedures. In parallel, other sectoral regulators should support compliance, oversight, and coordination in areas related to broadcasting, digital content, and platform regulation. Oversight and accountability must be reinforced through the National Human Rights Commission (NHRC), which should monitor adherence to constitutional protections and international human rights obligations in digital governance, particularly regarding freedom of expression, privacy, and non-discrimination. Collectively, effective coordination among these institutions, alongside civil society organizations, legal aid providers, and research bodies, is essential to establishing a coherent, rights-based, and survivor-centered national response to TFGBV.

Ms. Syeda Samara Mortada
Partnership and Coordination Analyst, UN Women, is addressing the National Dialogue on TFGBV in Dhaka

Summary of Legal Reform Recommendations

Reform Area	Proposed Action	Lead Agency
Legal Definition	Introduce comprehensive TFGBV law defining technology-enabled violence	Ministry of Law, Justice & Parliamentary Affairs (MoLJPA)
Harmonization	Align TFGBV provisions across cyber, penal, and privacy laws	MoICT, MoWCA and MoLJPA
Platform Accountability	Mandate local compliance and transparency reports from social media platforms	BTRC, MoICT
Institutional Strengthening	Create specialized TFGBV police and judicial units	Bangladesh Police, Judiciary
Cross-Border Cooperation	Develop regional agreements on TFGBV under SAARC	Ministry of Foreign Affairs

Ms. Khushi Kabir, Coordinator Nijera Kori, addressed the National Dialogue on TFGBV in Dhaka

Ms. Sharmeen S Murshid, Former Advisor, MoWCA, graced the National Dialogue on TFGBV as the Chief Guest

5. Platform Accountability and Regulation

Digital platforms and technology companies are central actors in shaping contemporary online environments. Their governance structures, algorithmic systems, and content moderation practices significantly influence whether digital spaces function as sites of participation and empowerment or as arenas of exclusion and harm. While these platforms offer critical avenues for communication, economic activity, and civic engagement, they often become key enablers of TFGBV unintentionally or unknowingly. In the absence of robust accountability mechanisms, platform design choices and enforcement gaps can amplify abuse, normalize misogyny, and undermine women's safety. Strengthening platform accountability and regulatory oversight is therefore a critical policy priority for Bangladesh's pursuit of a safe, inclusive, and rights-based digital ecosystem.

5.1 Role of Online Platforms in TFGBV

Social media and messaging platforms, most notably Facebook, TikTok, Instagram, and YouTube, constitute the primary digital spaces where TFGBV occurs in Bangladesh. Perpetrators exploit anonymity, inconsistent moderation practices, and algorithmic amplification to harass, intimidate, or defame women and gender-diverse individuals. Evidence suggests that harmful gendered content often spreads more rapidly than corrective or protective narratives, driven by engagement-based algorithms that privilege sensationalism over safety. In Bangladesh, the dominance of global platforms presents dual challenges: limited local oversight over the application of platform policies and persistent language and cultural gaps in automated moderation systems. Bengali-language abuse, locally specific slurs, and culturally coded harassment are frequently under-detected, allowing patterns of abuse to persist with minimal intervention.

5.2 Principles for Platform Accountability

Ensuring digital safety requires a co-regulatory approach in which online platforms could share responsibility with the state and civil society actors in Bangladesh. Experts mentioned that platform accountability frameworks should be grounded in several core principles. Transparency is essential, requiring platforms to publish regular, gender-disaggregated reports on content moderation, takedowns, and complaint resolution. Accessibility must be ensured through user-friendly reporting tools that are multilingual, inclusive of persons with disabilities, and responsive to local contexts. Data responsibility demands robust data protection measures, compliance with Bangladesh's forthcoming Personal Data Protection Act, and the adoption of privacy-by-design standards. Algorithmic fairness requires platforms to assess and disclose how recommendation systems may amplify gendered disinformation or abuse, along with mitigation strategies. Finally, collaboration should be institutionalized through formal channels linking

platforms, regulators, and women's rights organizations to enable rapid response and survivor referral.

5.3 National Digital Safety and Accountability Charter

To implement platform accountability effectively, Bangladesh could take initiatives to establish a National Digital Safety and Accountability Charter (DSAC), a co-regulatory framework endorsed by the government, technology companies, civil society and other relevant actors. Although voluntary in nature, the Charter should be subject to regulatory oversight and defined performance benchmarks. Essential provisions should include mandatory, periodic reporting on TFGBV complaints, content removals, and response timelines as well. It must also include framework considering standardized escalation protocols connecting the Bangladesh Telecommunication Regulatory Commission (BTRC), law enforcement agencies, and other relevant platforms. Furthermore, the Charter should advocate for gender-responsive platform design, incorporating safety prompts, privacy nudges, and simplified reporting mechanisms, alongside digital citizenship campaigns co-developed with relevant actors including women leaders, influencers and civil society. Despite all these, the proposed charter must be consistent with emerging global standards, such as the EU Digital Services Act (2024) and the OECD Digital Safety Framework, balancing accountability with the protection of freedom of expression.

5.4 Algorithmic Transparency and Content Moderation

Algorithms have been playing a decisive role in shaping the visibility, reach, and persistence of online content, including harmful and gendered content in social media platforms. To mitigate algorithm-driven harm, Bangladesh should require independent algorithmic audits to identify gender bias, cultural blind spots, and amplification of abusive content. Platforms should be mandated to disclose the scope and limitations of their automated moderation systems, particularly regarding the detection of Bengali-language abuse and context-specific bullying. Establishing a Public Register of Digital Moderation Policies under BTRC would enhance transparency by tracking platform commitments, compliance records, and public complaints. In addition, partnerships with academic institutions and research organizations should be encouraged to facilitate independent assessments of the algorithmic impact on digital violence including TFGBV, contributing to evidence-based regulation and public trust.

5.5 Addressing AI-Driven Harms

The rapid expansion of generative artificial intelligence has introduced new and complex risks, including deepfake pornography, identity impersonation, and synthetic disinformation targeting women and gender-diverse individuals. Realizing these emerging threats towards digital safety and security, Bangladesh's regulatory response must evolve accordingly. AI misuse reporting mechanisms should be integrated within existing cybercrime units to systematically document

and respond to AI-enabled digital violence including TFGBV. Technology companies and developers should be required to adhere to gender-sensitive AI design principles, embedding safeguards against exploitation, bias, and misuse throughout the development lifecycle. Strategic partnerships with universities, AI research labs, and civil society organizations can support the development of deepfake detection tools and ethical guidelines. Furthermore, AI-specific offences related to synthetic abuse should be explicitly incorporated into revisions of the Digital Security Act to ensure legal accountability for emerging forms of harm.

5.6 Regional and Global Cooperation

Given the transnational nature of digital platforms and online abuse, Bangladesh's regulatory efforts must be situated within broader regional and global governance frameworks. Regional dialogue and cooperation can facilitate the harmonization of standards on online harms, data sharing, and enforcement mechanisms. Engagement with international initiatives such as **UN Women's Global Digital Compact** offers opportunities to advance feminist digital governance and rights-based approaches. Additionally, structured engagement with global technology companies through memoranda of understanding can strengthen cross-border cooperation on TFGBV response, content moderation, and data transparency. Such multilevel collaboration is essential to ensuring that national regulatory efforts remain effective within an interconnected digital landscape.

Professor Dr. Meghna Guhathakurta, Advisor, JNUS, attended a workshop on Prevention of TFGBV with the members of YWLF in Chattogram

6. Prevention through Education and Capacity Building

If the opinion of the human rights activists and civil society are to be believed, preventing TFGBV requires a paradigm shift from reactive, punitive responses toward proactive, preventive, and capacity-building strategies. Legal remedies alone are insufficient to address the structural and normative drivers of digital violence. A prevention-centered approach emphasizes education, awareness, and institutional preparedness to equip individuals, particularly women, girls, adolescent and youth, with the knowledge, skills, and confidence to navigate digital spaces safely. If we can strengthen digital resilience promoting ethical online engagement, prevention efforts would contribute to building trust, inclusivity, and accountability within Bangladesh's rapidly evolving digital ecosystem.

6.1 Building Digital Literacy and Responsible Online Behavior

Digital literacy may contribute to the effective prevention of online abuse which have been exacerbating by limited awareness of digital safety, privacy settings, consent, and risk mitigation. Addressing these gaps must require the systematic integration of digital literacy and cyber ethics education into both formal and informal learning settings in Bangladesh. Members of YWLF suggested that gender-sensitive digital safety modules should be embedded within the National Curriculum Framework at secondary and tertiary levels, complemented by community-based learning hubs in schools, universities, and local organizations. They further recommended for undertaking nationwide public awareness initiatives, such as a "Safe Digital Bangladesh" campaign, Peer-led mentorship models, including the training of young women as Digital Safety Ambassadors, in extending outreach to rural and marginalized communities. Together, these initiatives should combine practical skills development, such as account security, abuse reporting, and digital footprint management, with critical engagement on gender norms that sustain online harassment.

6.2 Strengthening Law Enforcement and Judicial Capacity

The effective enforcement of legal measures would depend on the technical competence and gender sensitivity of the actors engaged the field of law enforcement and justice sector. In Bangladesh, gaps in digital forensic capacity and limited understanding of gendered digital harms continue to impede survivor-centered justice. Addressing these challenges might require the institutionalization of specialized TFGBV training programs within the Bangladesh Police Academy and the Judicial Training Institute, focusing on digital evidence handling, AI-enabled abuse, and trauma-informed approaches. The development of gender-sensitive Standard Operating Procedures (SOPs) is essential to ensure confidentiality, non-discrimination, and the preservation of digital evidence. Investments in digital forensic infrastructure, including AI-assisted investigative tools, should be prioritized within cybercrime units. To enhance

accountability, performance indicators related to TFGBV case handling, resolution rates, and survivor satisfaction should be introduced across law enforcement and judicial institutions.

6.3 Mental Health and Psychosocial Support

Survivors of TFGBV frequently experience enduring psychological and social harm, including anxiety, depression, social withdrawal, and fear of re-engagement in digital spaces. Effective prevention and recovery therefore require the integration of **mental health and psychosocial support services** within national response mechanisms. Survivor help desks at police stations and digital complaint centers need to be introduced which should offer psychosocial counseling alongside legal aid, ensuring holistic support. Existing national helplines, such as 109 and 999, should be strengthened through the inclusion of trained digital safety counselors and clear referral pathways. Community-based counseling initiatives, implemented in partnership with NGOs, youth groups, and academic institutions, can further expand access to mental health support. There is a serious requirement of sensitization among media representatives on gender-responsive reporting on incidents of TFGBV. As such, responsible media engagement is also critical, as ethical reporting practices help prevent sensationalism, secondary victimization, and retraumatization of survivors. Media outlets, as influential agenda-setters, have a responsibility to promote gender-sensitive reporting and amplify survivor-centered narratives.

6.4 Civil Society and Private Sector Engagement

Civil society organizations, academic institutions, and private sector actors could play indispensable roles in TFGBV prevention and capacity building in Bangladesh. Civil society organizations are uniquely positioned to implement grassroots awareness initiatives, provide survivor support, and advocate for digital rights at the community level. The private sector can contribute by integrating digital safety and gender equality commitments into corporate social responsibility (CSR) frameworks, supporting mentorship programs, awareness campaigns, and technological innovation. Academic institutions can advance evidence-based prevention through research, curriculum development, and policy evaluation. Collaborative networks among these actors could enhance sustainability, extend reach beyond urban centers, and ensure that prevention efforts address the needs of rural, ethnic, and refugee communities.

6.5 Promoting Digital Safety Leadership and Youth Engagement

Youth engagement, particularly the leadership of young women, is central to sustainable TFGBV prevention. Empowering youth as digital safety advocates can shift social norms, challenge misogynistic narratives, and foster peer accountability within online communities. Initiatives such as the **Young Women Leaders Forum (YWLF)** provide valuable platforms for mentoring digital advocates and strengthening feminist leadership in digital spaces. Small-scale **innovation** can further incentivize youth-led solutions, including reporting tools, awareness applications, and community campaigns. Recognition mechanisms, such as digital safety awards or competitions

for schools and universities, can reinforce positive practices and encourage institutional commitment to online safety and ethical digital engagement.

6.6 Institutionalizing Prevention in National Policy Frameworks

For prevention efforts to be sustainable and scalable, TFGBV must be systematically embedded within national policy and planning frameworks. Awareness, education, and prevention strategies should be integrated into the National ICT Policy, National Education Policy, and the National Action Plan on Violence Against Women (NAP-VAW). is essential to ensure that digital inclusion initiatives explicitly address safety, equity, and gender justice. Dedicated budgetary allocations for digital safety and prevention programs within sectoral ministries will further institutionalize commitments and enable long-term implementation. Prevention represents the most sustainable and transformative response to TFGBV. Such an approach not only mitigates harm but also advances broader goals of gender equality, democratic participation, and rights-based digital development.

Mr. Shamsud Douza, Joint Secretary, Ministry of Public Administration atteneded the Media Advocacy Dialogue in Dhaka as the Chief Guest

Ms. Saeda Bani, Project Coordinator, Feminist Opportunities Now (FON)| CREA, addressed the session in the National Dialogue in Dhaka

7. Strategic Framework for Implementation

The digital policy or act in Bangladesh requires a coordinated, multisectoral strategy that should align legal, educational, institutional, and technological interventions to ensure that prevention, protection, and prosecution mechanisms function cohesively, backed by data, partnerships, and accountability. This strategic framework should envision a safe, inclusive, and rights-based digital Bangladesh where women, girls, and gender-diverse people can participate freely in online spaces without fear of violence or discrimination. Grounded in human rights and gender justice, this approach could emphasize a whole-of-society model, evidence-based policymaking, and multi-stakeholder collaboration involving state institutions, civil society, academia, media, and the private sector, with strong commitments to transparency and accountability.

7.1 Multi-Stakeholder Coordination Mechanism

A high-level coordination architecture in the form of a **National Task Force on Preventing Digital Violence including TFGBV** under the Chief Advisor's Office/Prime Minister's Office (PMO) is recommended to ensure political leadership, cross-ministerial coherence, and strategic oversight. The Task Force should include representation from key line ministries, regulatory bodies, law enforcement agencies, UN entities, development partners, private sector actors, and women's rights organizations. Its core functions should include guiding the development and execution of the national TFGBV strategy, facilitating inter-agency coordination and resource mobilization, monitoring progress on legal reform and platform accountability. This Multi-Stakeholder Coordination Mechanism should complement efforts at the district and national level to support localized implementation, community awareness, and monitoring, ensuring that national commitments translate into action at the grassroots level.

7.2 Financing and Resource Mobilization

Sustainable financing is critical to translating policy commitments into measurable outcomes. The framework therefore calls for the introduction of dedicated budget lines on Preventing Digital Violence including TFGBV within the Ministry of Women and Children Affairs (MoWCA) and the Ministry of ICT (MoICT), specifically earmarked for prevention, awareness, research, and capacity-building initiatives. In parallel, public–private partnerships should be leveraged to engage telecommunications companies and technology firms in supporting digital safety initiatives through corporate social responsibility (CSR) investments. Development partners and UN agencies can play a catalytic role by providing technical assistance and funding for research, training, and institutional strengthening. To foster innovation and community ownership, the establishment of small-scale innovation funds is recommended to support youth-led and grassroots digital safety solutions, particularly in underserved and high-risk communities.

7.3 Monitoring, Evaluation, and Learning (MEL)

A robust Monitoring, Evaluation, and Learning (MEL) framework is essential to ensure accountability, effectiveness, and adaptability in addressing digital violence including TFGBV. This framework should include the development of clear and measurable performance indicators tracking legal enforcement, reporting and response rates, public awareness levels, and digital literacy outcomes. An annual review mechanism could provide transparency on progress, identify implementation gaps, and inform policy adjustments. Independent evaluations conducted by academic institutions and civil society organizations should be institutionalized to assess the effectiveness and equity of interventions. Importantly, MEL processes must support adaptive learning, enabling policymakers to incorporate emerging evidence and respond proactively to evolving technological risks, including AI-driven harms.

7.4 Communication and Advocacy Strategy

Sustained communication and advocacy are critical to building political will, shaping public discourse, and reducing the stigma surrounding TFGBV. A comprehensive advocacy strategy should therefore combine **multi-platform public campaigns** promoting gender equality, digital safety, and ethical online behavior with targeted engagement of policymakers, youth groups, and media professionals. Regular national conferences, policy dialogues, and regional consultations can serve as platforms for knowledge exchange and consensus-building. Survivor-centered communication, grounded in ethical storytelling and informed consent, should be encouraged to humanize digital harms, challenge victim-blaming narratives, and amplify stories of resilience and resistance. Through strategic advocacy, TFGBV can be repositioned as a national development, governance, and human rights priority rather than a marginal or purely technical issue.

Mr. Sadiq M. Alam, Managing Director and COO, Metamorphosis, a distinguished tech company, addressed the advocacy dialoue in Dhaka

Conclusion

The rapid digital transformation offers significant opportunities for empowerment, innovation, and inclusive development, but it has also reinforced existing gender inequalities in online spaces, particularly through technology-facilitated gender-based violence (TFGBV). TFGBV is not simply a cybercrime; it is a gendered human rights issue that requires coordinated, systemic, and rights-based responses.

Ensuring a safe and equitable digital Bangladesh demands a unified national framework that integrates prevention, protection, and prosecution. This includes establishing strong data systems such as a National TFGBV Observatory, undertaking harmonized legal reforms to address emerging digital harms like deepfakes, cyberflashing, and gendered disinformation, and strengthening platform accountability through co-regulation, transparency, and algorithmic oversight. Equally important are the institutionalization of digital literacy and ethics education, survivor-centered justice mechanisms, and the development of an AI and Gender Ethics Framework to ensure that technological innovation promotes equality rather than harm.

Achieving these objectives will require sustained collaboration among government institutions, regulators, the private sector, academia, media, and civil society. Digital gender equality must be recognized not only as a moral imperative but also as a strategic foundation for realizing Bangladesh's Vision 2041 and Smart Bangladesh goals.

Dr. Monira Ahsan, Research Consultant, is discussing in an FGD with the members of YWLF in Chattogram

JNUS

JAGO NARI UNNAYON SANGSTHA

Our Location
Ramu College Gate, Ramu
Cox's Bazar, Bangladesh.

Get in Touch
+88 01823 929 075

jagonariunnayon@gmail.com

www.jagonariunnayon.org