TECHNOLOGY, PEOPLE AND POLICY

Papers from the Tech Policy Fellowship 2024

Volume III

digitally right

TECHNOLOGY, PEOPLE AND POLICY

Papers from the Tech Policy Fellowship 2024

Volume III

digitally right

Technology, People and Policy
Papers from the Tech Policy Fellowship
Volume III

Editor
Abdullah Titir

Layout
Arka

Publisher
Digitally Right Limited

First published in April 2026
Second published in July 2026

Disclaimer

The research for the papers produced under the Tech Policy Fellowship, 2024, were conducted between March to September, 2025. Readers are advised that the regulatory landscape has undergone significant changes since the conclusion of this fellowship. The legislation, policies, and frameworks analyzed within these papers reflect the laws in effect during that specific period and may not represent current legal standing.

Furthermore, the views, analyses, concerns raised, legal interpretations, conclusions drawn, and recommendations proposed in these publications are solely those of the respective authors'. They do not necessarily reflect the official positions, or views of Digitally Right.

© Digitally Right Limited

Contents

	Foreword	**04**
1	**Nabangsu Chakma** THE 'NATIONAL SECURITY EXEMPTION' The PDPO 2025 and Its Implications	**06**
2	**Nazifa Muniyat Quader** LIABILITY OF TELCOS FOR HUMAN RIGHTS VIOLATIONS Case Study of Internet Shutdowns in Bangladesh	**27**
3	**Afrida Samiha Nabilah** WOULD COMMUNITY NOTES WORK IN BANGLADESH? Tackling Political and Gender-Based Misinformation	**39**
4	**Saraban Tahura Zaman** CHALLENGES IN ACCESSING JUSTICE Tech Facilitated Gender-based Violence in Bangladesh	**58**
5	**Tabassum Nuha** CYBER PROTECTION ORDINANCE 2025 AND THE POLITICS OF CONSENT Rethinking Online Intimacy, Gender, and Law in Bangladesh	**66**
	About the Authors	**78**

Foreword

The rapid evolution of digital technologies continues to reshape how societies function, govern, and express themselves. As Bangladesh navigates an increasingly complex digital landscape, the need for informed, critical, and rights-based engagement with technology policy has never been more urgent. Building on the success of previous cohorts, Digitally Right continued the Tech Policy Fellowship, 2024 to further strengthen the capacity of emerging leaders to engage with these challenges in meaningful and impactful ways.

The 2024 fellowship brought together a diverse group of young and mid-career professionals from law, academia, and civil society. Over the course of the program, fellows engaged in rigorous learning through expert-led sessions, collaborative discussions, and sustained mentorship. The fellowship not only deepened their understanding of global and local tech policy dynamics but also supported them in producing original research that contributes to Bangladesh's growing digital rights discourse.

This year's research reflects the urgency and complexity of contemporary policy debates. Fellows critically examined the implications of the 'national security exemption' under the Personal Data Protection Ordinance, 2025, particularly in relation to the right to privacy. They explored the role and liability of telecommunications companies in enabling internet shutdowns, raising important questions about corporate accountability and human rights. The intersection of law, gender, and technology was a key focus, with research unpacking the Cyber Protection Ordinance 2025 and its implications for consent, online intimacy, and gender justice.

Other studies addressed platform governance and accountability, including an analysis of Meta's Community Notes and its effectiveness in countering political and gender-based misinformation in the Bangladeshi context. The pervasive issue of technology-facilitated gender-based violence was also examined, highlighting systemic barriers to accessing justice and the need for survivor-centered legal and policy responses.

Together, these research papers underscore the critical intersections of technology, power, and rights. They offer timely insights into the risks and opportunities that define Bangladesh's digital future and contribute to broader regional and global conversations on technology governance.

We deeply appreciate the mentorship provided by Dr. Mohammad Ershadul Karim, Senior Lecturer, Faculty of Law, University of Malaya, Mohammad Pizuar Hossain, Senior Lecturer at the Department of Law, East West University, and Shubha Kayastha, Academic Tutor, School of Education, La Trobe University. Their guidance played a crucial role in shaping the fellows' research. Our sincere thanks go to Abdullah Titir, Head of Research at Digitally Right Limited, for her meticulous editorial review of the reports.

We are especially thankful to our knowledge partner, Access Now, for their continued collaboration and support. Together, these contributions strengthened the intellectual depth and quality of the fellowship research papers.

We also extend our appreciation to the fellows themselves, whose dedication, curiosity, and commitment to advancing digital rights have made this body of work possible.

We hope this publication will serve as a valuable resource for researchers, policymakers, practitioners, and advocates, and that it will inspire continued dialogue and action toward building a more inclusive, rights-respecting, and accountable digital ecosystem in Bangladesh.

Miraj Ahmed Chowdhury
Founder & Managing Director
Digitally Right

THE 'NATIONAL SECURITY EXEMPTION'

The PDPO 2025 and Its Implications

Nabangsu Chakma

Abstract

As governance, commerce, and communication become increasingly digitized, data protection laws are vital to safeguarding individuals' right to privacy. Bangladesh's Draft Personal Data Protection Ordinance, 2025 (DPDPO 2025) seeks to regulate the collection, storage, and use of personal data. However, its inclusion of broad national security exemptions raises significant concerns regarding potential governmental overreach and the erosion of privacy rights. This research critically examines the legal principles governing national security exemptions and evaluates the extent to which these are reflected in the DPDPO 2025. It further explores the implications of such exemptions for privacy protection, analyzing whether the Ordinance strikes an appropriate balance between national security and individual rights, or instead creates avenues for unchecked surveillance. By situating Bangladesh's draft framework within comparative global standards, the study highlights the necessity of narrowly tailored national security exemptions and related provisions that safeguard state interests without undermining fundamental rights. The findings aim to contribute to the broader discourse on data protection in Bangladesh and offer policy insights to enhance accountability, transparency, and alignment with international privacy standards.

Keywords: *Personal Data Protection, Right to Privacy, National Security Exemptions, Draft Personal Data Protection Ordinance 2025, Government Surveillance, Data Processing*

1. INTRODUCTION

In response to the growing importance of personal data protection and in line with global developments, Bangladesh initiated the drafting of its own data protection law in 2022. Following multiple rounds of revisions and consultations with stakeholders, including civil society organizations and digital rights advocates, the Cabinet approved the draft Act in November 2023, setting the stage for its submission to Parliament for final approval and anticipated enactment in 2024.[1]

The Act was expected to be tabled in Parliament in early 2024 for final approval and enactment. However, the draft law drew considerable criticism from rights groups for provisions that enabled government overreach, unchecked surveillance, and broad discretionary powers without adequate safeguards.[2] Despite widespread concern, the government largely retained these features, making minimal improvements in line with global best practices.

Before the law could be formally introduced in Parliament, Bangladesh experienced significant political upheaval during the July Uprising, which resulted in a regime change.[3] Consequently, the 2024 draft Act was shelved and never enacted into law. In the aftermath, an interim government led by Nobel Laureate Dr. Muhammad Yunus assumed power and revived efforts to formulate a data protection regime. This led to the introduction of a new draft titled the Draft Personal Data Protection Ordinance, 2025.[4]

While the 2025 draft differs from its predecessors in some structural and definitional aspects, many of the core concerns raised earlier remain unaddressed. Most notably, the ordinance retains broad exemptions on the grounds of national security, which effectively grant the government

1 See 'Draft Data Protection Act: Cabinet Okays It Giving Free Rein to Law Enforcers', *The Daily Star* (online, 28 November 2023) https://www.thedailystar.net/news/bangladesh/news/draft-data-protection-act-cabinet-okays-it-giving-free-rein-law-enforcers-3480656 ('Draft Data Protection Act'); 'Personal Data Protection Act Gets Cabinet Approval in Principle', *BSS* (online, 27 November 2023) https://www.bssnews.net/news-flash/160354.

2 See 'Draft Data Protection Act', *supra* note 1; Transparency International Bangladesh, *The Revised Draft Data Protection Act (DPA) 2023: Review and Recommendations in Light of Submissions on the Earlier Version* (Report, September 2023) 1–38 https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-Paper-on-Revised-Draft-Data-Protection-Act-Review-Recommendations.pdf; 'Data Protection Act: Constitutional Rights of Citizens Are at Risk', *The Daily Star* (online, 2 March 2023) https://www.thedailystar.net/news/bangladesh/news/data-protection-act-constitutional-rights-citizens-are-risk-3260756; Access Now & Tech Global Institute, *Submission on the Draft Data Protection Act, 2023*, (Submission and Recommendations, 26 October, 2023) 1–7 https://www.accessnow.org/wp-content/uploads/2023/10/Submission-on-the-Bangladesh-Data-Protection-Act-2023-Access-Now-and-Tech-Global-Institute.pdf.

3 In July 2024, mass protests led by students started with peaceful demonstrations against the unjust quota system in Bangladeshi government jobs. However, these nationwide protests quickly snowballed into a violent eruption of anger towards the 15-year-long autocratic rule of the iron lady, Sheikh Hasina, and her party, Awami League. When the Government began brutally cracking down on the protesters, people from all walks of life, frustrated by her tyrannical governance, unitedly rose against her. They defied curfew on August 5 and finally succeeded in ousting her and her party from power and the country. For details, see Anbarasan Ethirajan, 'How Bangladesh's Protests Ended Sheikh Hasina's 15-Year Reign', *BBC* (online, 5 August 2024) https://www.bbc.com/news/articles/c9033zpv0nvo; Anbarasan Ethirajan and Tessa Wong, 'Sheikh Hasina: The Pro-Democracy Icon Who Became an Autocrat', BBC (online, 6 August 2024) https://www.bbc.com/news/articles/cg3ee303yxpo; Partha Pratim Bhattacharjee and Zyma Islam, 'Hasina's Final Days Before the Fall', *The Daily Star* (online, 5 August 2025) https://www.thedailystar.net/news/bangladesh/news/hasinas-final-days-the-fall-3955566.

4 The Government has finalized the draft Ordinance, and it is ready to be officially promulgated. 'Govt Moves to Secure Personal Data with Ordinance Draft', *Dhaka Tribune* (online, 3 June 2025) https://www.dhakatribune.com/bangladesh/government-affairs/383062/new-law-in-works-to-safeguard-citizens%E2%80%99-personal.

sweeping powers to monitor and surveil citizens without sufficient legal safeguards. These provisions, which lack adequate oversight or independent checks, raise serious concerns regarding the protection of personal data and the broader right to privacy.

Bangladesh's historical misuse of digital laws, often employed to silence dissent, target opposition voices, and suppress free expression, underscores the urgency of scrutinizing these national security exemptions.[5] Unlike previous digital laws, the current draft Ordinance permits more extensive forms of surveillance, particularly over personal data. By allowing the state to limit privacy rights in the name of national security without codified protections or accountability mechanisms, the law poses a serious threat to civil liberties. Essential safeguards such as judicial oversight, codified principles obligating adherence to necessity, and proportionality are notably absent.

Given the country's poor track record in upholding human rights and protecting citizens from arbitrary intrusions into their private lives,[6] the Draft Ordinance demands special attention. Without clear limitations and checks on the state's power to invoke national security, the risk of abuse remains high. The potential for infringing upon the right to privacy is especially concerning in a political context where digital laws have frequently been weaponised.

This article aims to critically examine the national security exemption provisions embedded within the Draft Personal Data Protection Ordinance 2025, and assess their implications for individual privacy rights. Part 2 presents the theoretical framework for the analysis, outlining key concepts such as 'national security,' its legal 'exemption' status, and the scope and limitations of the right to privacy under international human rights law. Part 3 discusses the normative principles governing national security exemptions, particularly the standards of necessity and proportionality, and how they are implemented in global best practices. Part 4 offers a detailed analysis of the national security-related provisions in the 2025 draft Ordinance, identifying their legal scope, ambiguity, and potential for misuse. Part 5 explores the broader implications of these provisions on the right to privacy, especially in light of Bangladesh's documented history of using digital regulations for political repression. This section argues that the continued absence of adequate legal safeguards significantly undermines trust in the state's commitment to protect personal data. Finally, Part 6 concludes the discussion by summarizing the key findings and recommending urgent reforms to align the draft Ordinance with international human rights standards.

5 See generally Ali Riaz, T*he Unending Nightmare: Impacts of Bangladesh's Digital Security Act 2018* (Centre for Governance Studies, April 2022) 5–30; Amnesty International, *Bangladesh: Muzzling Dissent Online – Amend the Draconian Digital Security Act* (Report, 12 November 2018) 2–9 https://www.amnesty.org/en/documents/asa13/9364/2018/en/ ('Bangladesh: Muzzling Dissent Online'); Article 19, *Bangladesh: Analysis of Information Communication Technology Act* – Legal Analysis (Report, April 2016) 4–19 https://www.article19.org/data/files/medialibrary/38365/Bangladesh-ICT-Law-Analysis.pdf; Human Rights Watch, *No Place for Criticism: Bangladesh Crackdown on Social Media Commentary* (Report, May 2018) 1–89 https://www.hrw.org/sites/default/files/report_pdf/bangladesh0518_web.pdf; Amnesty International, Repackaging Repression: The Cyber Security Act and the Continuing Lawfare Against Dissent in Bangladesh (Report, 2024) 4–61 https://www.amnestyusa.org/wp-content/uploads/2024/08/Repackaging-Repression-The-Cyber-Security-Act-and-the-Continuing-Lawfare-Against-Dissent-in-Bangladesh.pdf *('Repackaging Repression')*.

6 See ibid.

2 THEORETICAL FRAMEWORK

2.1 What do 'National Security' and its 'Exemption' Constitute?

In general terms, 'national security' denotes a country's ability to defend itself from foreign threats of violence or attack.[7] For a long time, the notion of national security has been understood only in terms of a nation's military security, primarily focusing on military capabilities.[8] By non-military means, a nation can be threatened was inconceivable. Traditionally, at the center of the concept of 'national security' lay the idea of securing the state's physical existence and safeguarding it against any encroachment.[9]

The Heritage Foundation defines 'national security' as "the safekeeping of the nation as a whole. Its highest order of business is the protection of the nation and its people from attack and other external dangers by maintaining armed forces and guarding state secrets."[10] Today, the concept of 'national security' extends beyond the protection of national sovereignty, which includes airspace and territorial waters, and safeguarding the lives of the people and their property. It also encompasses economic security, energy and natural resources, sociopolitical stability, cultural preservation, environmental protection, cybersecurity, as well as health and food security.[11]

'National security exemption' or 'exception' refers to a provision or clause often found across many constitutions, legislations, and international agreements worldwide. This clause generally empowers the government of a state to override specific effects of such constitutions, legislations, and agreements to protect its national security interests. While Constitutions serve as the primary foundation for guaranteeing citizens' rights within a state, they often permit the regulation of these rights on the grounds of national 'sovereignty,' 'integrity,' or 'security.' These terms are frequently used interchangeably to justify what is broadly referred to as a national security exemption or exception.

For example, the Indian Constitution under Article 19 ensures a few fundamental rights, which include freedom of speech and expression, peaceful assembly, freedom of movement, among others, while under its clauses (2), (3), and (4), it imposes restrictions on these fundamental rights based on "in the interests of sovereignty and integrity of India."[12] These national security exemption clauses allow the government of India to override and limit the rights when national security concerns arise. Similarly, in Bangladesh, the fundamental rights of freedom of thought, conscience, and speech, along with protection of the home and privacy of correspondence and communication, can be restricted by the government "in the interests of the security of the State" under Articles 39 and 43 of the Constitution of Bangladesh.[13]

7 See *Collins English Dictionary* (online at 13 June 2025) 'National Security' https://www.collinsdictionary.com/dictionary/english/national-security.

8 Joseph J Romm, *Defining National Security: The Nonmilitary Aspects* (Council on Foreign Relations Press, 1993) vii; Kim R Holmes, 'What is National Security' in Dakota L. Wood (ed), *2015 Index of U.S. Military Strength: Assessing America's Ability to Provide for the Common Defense* (The Heritage Foundation, 2015) 19.

9 Donald M Snow, *National Security for a New Era* (Routledge, 5th ed, 2016) 7.

10 Holmes (n 8) 23.

11 ibid 19-20; Anton Grizold, 'The Concept of National Security in the Contemporary World' (1994) 11 (3) *International Journal on World Peace* 37, 41.

12 *Constitution of India* art 19.

13 *Constitution of the People's Republic of Bangladesh* arts 39, 43. Article 39 guarantees freedom of thought, conscience, and speech, while Article 43 protects an individual's privacy rights in their home, correspondence, and other forms of communication.

It is evident that national security exemption clauses are most frequently applied to limit the rights to freedom of expression and privacy. These fundamental rights, which are said to be two sides of the same coin and inextricably intertwined,[14] often pose significant constraints on a government's ability to conduct surveillance and gather intelligence, particularly in situations involving potential threats to national security. The underlying rationale for such exemptions is that they remove these legal and procedural barriers, thereby enabling the state to monitor, intercept, and potentially control data, speech, and communication in order to prevent threats such as terrorism, cyberattacks, and foreign interference.

Accordingly, most privacy and data protection laws include national security exemptions. Even the EU General Data Protection Regulation (GDPR), widely regarded as the gold standard in data protection, contains such a provision.[15] Likewise, the UK Data Protection Act of 2018,[16] India's Digital Personal Data Protection Act of 2023 (DPDPA),17 Sri Lanka's Personal Data Protection Act of 2022 (PDPA),[18] and Bangladesh's draft Personal Data Protection Ordinance of 2025 (PDPO)[19] feature such provisions or clauses.

2.2 Ambits and Limits of the Right to Privacy

Privacy is a broad concept. The concept has varied across different cultures and historical periods, expanding beyond the idea of a concrete private domain or property to include the protection of personal thoughts and ideas in this digital age.[20] The idea of privacy can encompass privacy related to information (*i.e.* protection of personal data from unauthorized access and breaches), body (*i.e.* safeguarding of physical body from unwanted physical searches and medical tests), communications (*i.e.* confidentiality for all forms of communications irrespective of the technology and methods) and territory (*i.e.* preventing unauthorized intrusion in personal spaces, including homes, workplaces, and public areas).[21] In its dictionary definition, the Merriam-Webster Dictionary defines privacy as "the quality or state of being apart from company or observation" and "freedom from unauthorized intrusion."[22]

Privacy is widely recognized as a fundamental human right. It is understood as the expectation that individuals are entitled to a personal domain of freedom, growth, and interaction, a 'private sphere' where they can live independently or engage with others, shielded from state intrusion and unwarranted interference by others.[23] It

14 Carly Nyst, 'Two Sides of the Same Coin – The Right to Privacy and Freedom of Expression' (Blog Post, Privacy International, 7 October 2013) https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression.

15 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L 119/1, art 23 (*'GDPR'*).

16 Data Protection Act 2018 (UK) s 26.

17 Digital Personal Data Protection Act 2023 (India) ss 7(c), 17(2)(a).

18 Personal Data Protection Act 2022 (Sri Lanka) ss 17(2)(a), 25(7), 40(a) (*'PDPA'*).

19 Draft Personal Data Protection Ordinance 2025 (Bangladesh) ss 5(6)(b), 48(1) (*'DPDPO'*).

20 Jackson Adams and Hala Almahmoud, 'The Meaning of Privacy in the Digital Era' (2023) 15(1) *International Journal of Security and Privacy in Pervasive Computing* 1, 2.

21 David Banisar and Simon Davies, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice* (Report, Privacy International, 2000) https://gilc.org/privacy/survey/intro.html.

22 Merriam-Webster (online at 13 June 2025) 'Privacy' https://www.merriam-webster.com/dictionary/privacy.

23 See Lord Lester and David Pannick (eds), *Human Rights Law and Practice* (Butterworths, 2nd ed, 2004) [4.82]; Martin Scheinin, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, UN Doc A/HRC/13/37 (28 December 2009) [11].

enables, supports, protects, and is intrinsically linked to the exercise of other essential rights, such as freedom of expression, thought, religion, assembly, and association.[24] Because of the significance of the right to privacy, it has been enshrined in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) as a core human right. Article 12 of the UDHR and Article 17 of the ICCPR state, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[25] Inspired by these Articles, Bangladesh also incorporated the right to privacy as a fundamental right in Article 43 of its Constitution, which reads, "Every citizen shall have the right, subject to any reasonable restrictions imposed by law in the interests of the security of the State, public order, public morality or public health – (a) to be secured in his home against entry, search and seizure; and (b) to the privacy of his correspondence and other means of communication."[26]

Despite the right to privacy being a fundamental right, it is not an absolute one. Many Constitutions and laws worldwide impose limits or restrictions on exercising this right. These limits are typically imposed in the interests of national security, sovereignty, and integrity of the state, friendly relations with foreign states, public order, morality, or health, or in relation to contempt of court, defamation, or incitement to an offence.[27] These restrictions must be reasonable, implying they cannot be arbitrary, and balanced against such legitimate interests.[28]

Such a limit on the right to privacy on the basis of security may seem to suggest that security trumps privacy, meaning that in conflicts between the two, security often takes precedence over the right to privacy. However, both privacy and security are generally commensurable, meaning they can be compared and weighed, though not always easily or clearly. In practice, the importance of the interests involved, the number of people affected, and the proportionality of the trade-off all influence which right should prevail. Thus, while security may often outweigh privacy in matters of life, safety, or survival, each case requires careful, context-sensitive evaluation.[29]

24 See *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, UN Doc A/HRC/39/29, 39th sess (3 August 2018) [11]; *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, UN Doc A/HRC/23/40, 23rd sess (17 April 2013) [24]–[27]; *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, UN Doc A/HRC/29/32, 29th sess (22 May 2015) [15]; *Joint Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association and the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions on the Proper Management of Assemblies: Note by the Secretariat,* UN Doc A/HRC/31/66, 31st sess (4 February 2016) [73]–[78]; *Rights to Freedom of Peaceful Assembly and of Association: Note by the Secretary-General*, UN Doc A/72/135, 72nd sess (14 July 2017) [47]–[50]; *The Right to Privacy in the Digital Age*, HRC Res 42/15, 42nd sess, UN Doc A/HRC/RES/42/15 (7 October 2019).

25 *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) art 12; *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

26 *Constitution of the People's Republic of Bangladesh* (Bangladesh) art 43.

27 See, eg, *Constitution of India* art 19; *Constitution of the People's Republic of Bangladesh* (Bangladesh) arts 39, 43.

28 ibid.

29 Kenneth E Himma, 'Privacy Versus Security: Why Privacy is Not an Absolute Value or Right' (2007) 44(4) *San Diego Law Review* 857, 872–6.

3. PRINCIPLES GOVERNING NATIONAL SECURITY EXEMPTION

Interference with human rights is permitted when prescribed by law—that is, when it is authorized by legislation, but this does not grant governments a blank cheque to restrict rights at their whim.[30] Under international human rights law, any limitation on the right to privacy must meet the standards of necessity and proportionality.[31] Therefore, to ensure that any restrictions on the right to personal data protection and the right to privacy remain legitimate and prevent arbitrary interference, the national security exemption provision must be governed by the principles of "necessity and proportionality". The burden of proof is upon the Government to show that the restriction or interference on the rights is necessary and proportionate to the protection of national security interests.[32]

It is deeply concerning that the Draft Personal Data Protection Ordinance of 2025 does not include any of these standards. However, the insertion of necessity and proportionality as standards governing national security exemption is found in the General Data Protection Regulation (GDPR). Article 23(1)(a) of the GDPR explicitly allows Union or Member State law to limit certain rights and obligations of data subjects—which encompass core data subject rights such as access, rectification, erasure, and objection (Articles 12 to 22)—on the ground of national security provided such limitation respects the essence of fundamental rights and freedoms and adheres to the principles of necessity and proportionality.[33] Influenced by the GDPR, the Sri Lankan Data Protection Act of 2022 and the Albanian Data Protection Law of 2024 permit any exemption, restriction, or derogation in the interest of national security, specifically when such measures are necessary and proportionate in a democratic society.[34]

3.1 Necessity

The "principle of necessity" is one of the two fundamental standards that must be followed when restricting any human rights. This principle also applies to the right to the protection of personal data and privacy rights. Any restrictions on privacy or personal data protection that involve government surveillance must meet the necessary standard, and they must be aimed at a legitimate objective.[35] National security is considered a legitimate objective. In the European Union, any surveillance, intrusion, interference, or restriction on the grounds of national security is allowed only when it is "necessary in a democratic society."[36] This

30 See ECHR art 5(1); UDHR art 29(2).

31 See Privacy International, 'Legality, Necessity and Proportionality' https://privacyinternational.org/our-demands/legality-necessity-and-proportionality (accessed 13 June 2025); Human Rights Committee, General Comment No 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, UN Doc CCPR/C/21/Rev.1/Add.13 (26 May 2004) [6]; Human Rights Council, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights, UN Doc A/HRC/27/37 (30 June 2014) [23]–[27] ('Right to Privacy Report').

32 See Right to Privacy Report (n 31) [25].

33 *GDPR (n 15) art 23(1)(a).*

34 Personal Data Protection Act 2022 (Sri Lanka) s 40; Law No 18/2024 on Personal Data Protection (Albania) art 21.

35 Geneva Academy of International Humanitarian Law and Human Rights, T*he Right to Privacy in the Digital Age: Meeting Report* (Meeting Report, 24–25 February 2014) 2 https://www.geneva-academy.ch/joomlatools-files/docman-files/ReportThe%20Right%20to%20Privacy%20in%20the%20Digital%20Age.pdf.

36 See *ECHR*, *supra* note 30, art 8; *GDPR* (n 15) art 23. Although the principle that state restrictions on the right to privacy must be 'necessary in a democratic society' originates from Europe and applies specifically under the European Convention on Human Rights, it should also be adopted by other democratic countries, as it offers a reasonable and balanced standard for limiting privacy rights and ensuring data protection.

standard is reasonable and ju stified, and an inspiration to be followed in a democratic country, as it establishes that measures taken in the name of national security must serve the democratic government of a state.

In the case of *Handyside v. the United Kingdom* (1976), a foundational case for European human rights law, concerning the right to freedom of expression, the Strasbourg Court stressed that "necessary" is not as loose or flexible as terms like "admissible," "useful," "reasonable," or "desirable."[37] It held that necessity implies a "pressing social need."[38] This interpretation was reaffirmed in *The Sunday Times v. the United Kingdom* (1979), where the Court explicitly referred back to *Handyside*.[39] The same standard was reiterated in *Breyer v. Germany*, a case concerning privacy rights, where the Court held that "[a]n interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and if it is proportionate to the legitimate aim pursued."[40] To implement surveillance measures for national security purposes, states are allowed to "enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security."[41] However, this power cannot serve as arbitrary interference, amounting to unfettered discretion.[42] The surveillance or restrictive measures under the discretionary power of a wide margin of appreciation must be subject to judicial review to maintain the interference within the limits of what is "necessary in a democratic society."[43]

The test of "necessary in a democratic society" has evolved further into a higher standard of necessity called the "strictly necessary" test. It implies that the action or interference for national security must be indispensable, not just reasonable or useful. In *Szabó* and *Vissy v. Hungary* (2016), a case concerning privacy rights violation due to secret surveillance for national security aims, the *ECtHR* taking into account the nature of such intrusion and the modern surveillance capabilities to intrude a person's privacy held that "the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects," first if it is only strictly necessary for the "safeguarding the democratic institutions" and second for obtaining "vital intelligence" in an individual operation.[44]

Furthermore, the Court opined that "any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal."[45] Similarly, extending the right to respect for private life to personal data protection, the CJEU has held that "the right to respect for private life requires that derogations and limitations in relation to the protection of personal data must apply only in

37 *Handyside v United Kingdom* (1976) 1 EHRR 737 [48].

38 ibid.

39 *The Sunday Times v United Kingdom* (1979) 2 EHRR 245 [59].

40 *Breyer v Germany* (European Court of Human Rights, Application No 50001/12, 30 January 2020) [88].

41 Weber and Saravia v Germany (European Court of Human Rights, Application No 54934/00, 29 June 2006) [106].

42 ibid [94].

43 *Kennedy v the United Kingdom* (European Court of Human Rights, Application No 26839/05, 18 May 2010) [154].

44 *Szabó* and *Vissy v Hungary* (European Court of Human Rights, Application No 37138/14, 12 January 2016) [73].

45 ibid.

so far as is strictly necessary."[46] The surveillance measures in this regard must be the least intrusive means available to achieve the legitimate aim.[47] Ultimately, in data protection law, the necessity test should be conducted through a context-specific, fact-based analysis, reflecting both the substantive provisions of the measure in question and the legitimate aim it is intended to serve.[48]

3.2 Proportionality

In the context of privacy rights and data protection, the principle of proportionality aims to balance individual rights with the legitimate interests of national security.[49] The proportionality of a restrictive measure is assessed in three steps: (i) appropriateness; (ii) necessity; and (iii) proportionality *stricto sensu* (strict sense).[50] First of all, the measure must be appropriate to achieve the legitimate aim it intends to achieve and safeguard the legitimate interest it seeks to protect.[51] It involves ensuring that any restrictions on rights are appropriate and justified by the benefits those restrictions intend to achieve.[52] It has also been referred to as the concept of "adequacy" by the Inter-American Court of Human Rights.[53] This standard is similar to the Canadian concept of "rationally connected," which entails that the measure must be effective in attaining the legitimate objective pursued.[54] Such a measure must also be fair and not arbitrary to the rights that will be limited.[55] Secondly, the necessity test will be conducted to assess whether the measure will be a necessity to get the projected result and whether the measure will be the least intrusive one to get the desired result.[56] Finally, the test of proportionality *stricto sensu* is a result-oriented test that seeks to balance between the benefits gained by the restriction of a right and the harm caused by such a

46 See *Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR v Land Hessen* (Court of Justice of the European Union, 9 November 2010) [77]; *Case C-473/12 Institut professionnel des agents immobiliers (IPI) v GE* (Court of Justice of the European Union, 7 November 2013) [39]; *Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (Court of Justice of the European Union, 8 April 2014) [52]; *Case C-212/13 Ryneš v Úřad pro ochranu osobních údajů* (Court of Justice of the European Union, 11 December 2014) [28]; *Case C-362/14 Maximillian Schrems v Data Protection Commissioner* (Court of Justice of the European Union, 6 October 2015) [92].

47 See European Data Protection Supervisor, *Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (2017) 5 ('EDPS, *Toolkit*'); *Roman Zakharov v Russia* (European Court of Human Rights, Application No 47143/06, 4 December 2015) [260].

48 See *Roman Zakharov* (n 47) [232]; *Szabó* (n 44) [57] ("The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law."); EDPS, *Toolkit* (n 47) 5, 8.

49 See Jonida Milaj, 'Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance' (2016) 30(3) *International Review of Law, Computers & Technology* 115, 116–17.

50 Antonio Troncoso Reigada, 'The Principle of Proportionality and the Fundamental Right to Personal Data Protection: The Biometric Data Processing' (2012) 17(2) *Lex Electronica* 1, 16.

51 See *Scheinin, Report on Human Rights and Counter-Terrorism* (n 23) [17].

52 See Kevin Macnish, 'An Eye for an Eye: Proportionality and Surveillance' (2015) 18(3) *Ethical Theory and Moral Practice 529, 532.*

53 *Fontevecchia and D'Amico v Argentina* (Merits, Reparations and Costs) (Inter-American Court of Human Rights, Series C No 238, 29 November 2011) [53].

54 Electronic Frontier Foundation and Article 19, *Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance – Background and Supporting International Legal Analysis* (Report, May 2014) 46 https://www.article19.org/data/files/medialibrary/37564/N&P-analysis-2-final.pdf.

55 *R v Oakes* [1986] 1 SCR 103, [70].

56 See Scheinin, *Report on Human Rights and Counter-Terrorism* (n 23) [17]; Tor-Inge Harbo, 'The Function of the Proportionality Principle in EU Law' (2010) 16(2) *European Law Journal* 158, 165.

restriction on the right.[57] It requires that the harm caused by limiting or interfering with a right should not outweigh the advantages that the limitation is meant to provide.

A restrictive measure is not proportional in the strict sense if it fails to gain benefits surpassing the harm caused to the right in this balancing test. Therefore, ensuring proportionality in restricting privacy rights and data protection for the legitimate objective of national security will require that the restriction be appropriate to achieve the specific goal of safeguarding national security, meaning it must have a clear and direct connection to the threat being addressed. Moreover, it must be both necessary, where no less intrusive measure would suffice, and balanced, ensuring that the benefits to national security clearly outweigh the adverse impact on the protected rights.

4. 'NATIONAL SECURITY EXEMPTION' UNDER THE DRAFT PERSONAL DATA PROTECTION ORDINANCE, 2025

The draft Ordinance *prima facie* appears to adopt a rights-oriented approach in data processing. In this context, processing means "any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, transfer, adaptation or alteration, retrieval, consultation use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, destruction or erasure of the personal data."[58]

The preamble emphasizes that the Ordinance has been prepared with a view to making "provisions for processing of personal data of a person for the purposes of legitimate use ensuring privacy, confidentiality, and security incorporating principles being reflective of best practices, and recognizing the personal data as personal right of a data-subject."[59] The preambular text denotes that the Ordinance aims to establish a regulatory legal framework for the processing of personal data in a manner that serves legitimate purposes, while safeguarding the privacy, confidentiality, and security of individuals. It also underscores the incorporation of principles aligned with international best practices and, notably, affirms the recognition of personal data as an inherent personal right of the data subject. This reflects a normative commitment to both regulatory oversight and the protection of individual autonomy in the digital age.

In this regard, the draft seems to have emphasized the necessity of consent for processing personal data. Section 5(1)-(2) specifies that data processing of personal data requires consent that must be freely given, specific, clear, and revocable by the data subject. However, under Section 5(6) such a requirement for consent is absent. The provision reads, "A data-fiduciary may process personal data of a data subject, in such manner as may be prescribed by regulations, if the processing is necessary for following legitimate uses, namely: —

a. for the public interest;

b. for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in Bangladesh or in the interest of sovereignty and integrity of Bangladesh or security of the State;

57 Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press, 2012) 340, 342.

58 *DPDPO* (n 19) s 2(i).

59 ibid Preamble.

c. for fulfilling any obligation under any law, for compliance with any judgment or decree or order issued under any law for the time being in force in Bangladesh;

d. for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order;

e. for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Fiduciary who is an employee."

Thus, among the various grounds enumerated in clauses (a) to (e), clause (b)—which relates to national security or the security of the State—stands out as a key legitimate basis upon which a data fiduciary may lawfully process the personal data of a data subject. Such processing must only adhere to the procedures prescribed by the relevant regulations and must be necessary for the pursuit of legitimate national security objectives. Therefore, Section 5(6)(b) underpins that under 'national security' grounds, an exemption is created, because of which data collection and examination can be allowed without the data subject's knowledge or consent, as long as it follows the procedures specified by regulations.

Section 48 also contains national security exemption, which states "(1) For the purposes of this Ordinance, the Government may, from time to time, issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of Bangladesh, the security of the state, friendly relations with foreign states or public order or public health.

(2) Without prejudice to other provisions of this Ordinance, the Authority shall be bound to comply with such directions of the Government in the performance of its duties under this Ordinance."

Thus, Section 48(1) empowers the Government to issue directions to the National Data Governance and Interoperability Authority [hereinafter as Authority][60] as it deems necessary on broadly framed and undefined national security interest grounds. Section 48(2) further mandates that the Board is legally bound to comply with such directions in the performance of its duties under the Act. This provision strips the Authority of any discretion or institutional independence to question or refuse government directives, even where they may conflict with the rights of data subjects. Moreover, the Authority has been turned into a subordinate institution that the Government can fully control.

In effect, Section 48 grants the Government sweeping authority to direct and potentially override the data protection framework based on vaguely defined grounds, without any checks or independent oversight. While Sections 5(6)(b) and 48 both invoke national security as a basis for exemption, they provide no substantive standards, safeguards, or procedural requirements to ensure that such exemptions are necessary, proportionate, and subject to accountability. More alarmingly, the threat to the right to privacy becomes starkly evident when these provisions are read together. The legal vacuum opens the door to arbitrary interference with personal data, fundamentally undermining the right to privacy guaranteed in the Constitution of Bangladesh and the ICCPR.

60 ibid s 2(e) (defines "Authority" as the National Data Governance and Interoperability Authority established under the National Data Governance and Interoperability Authority Ordinance, 2025 (Bangladesh)).

5. POTENTIAL IMPACTS OF NATIONAL SECURITY EXCEPTION ON THE RIGHT TO PRIVACY IN BANGLADESH

5.1 Patterns of Abuse of Digital Laws and Reasons for Concerns

History shows that through clever drafting of legislation that lacks robust legal safeguards for its citizens, the Government of Bangladesh has created broad and unfettered opportunities to exploit legal loopholes for the furtherance of authoritarian rule. These seemingly rights-protective laws, filled with overreaching provisions and clauses, enabled systemic violations of citizens' rights.

A prime example is the Information and Communication Technology (ICT) Act of 2006, which was adopted to prevent cybercrimes and regulate digital communications, but was instead used to curtail the right to freedom of expression. Following the 2013 amendment, particularly the inclusion of the infamous section 57—which allowed non-bailable arrest without a judicial warrant, imprisonment for fourteen years and a fine up to BDT one crore for publication of fake, obscene, or defamatory information disrupting law and order, damaging the State's reputation, or hurting religious sentiments—a total of 1665 cases were filed, and approximately 747 cases were based on section 57 alone.[61] Hundreds of people, including prominent journalists, human rights defenders, opposition members, activists, academics, and ordinary people, were targeted and arrested under section 57 for criticizing the government and its policies, online trolling key ruling party figures, making corruption allegations, and hurting religious sentiments, significantly limiting criticism and dissent—violating the citizens' right to freedom of expression.[62]

In 2018, the Act was repealed and replaced by the Digital Security Act, supposedly for novel objectives to ensure digital security and identity protection, to address crimes such as unauthorized access to digital systems, digital forgery and fraud, dissemination of propaganda, disinformation, and defamation, identity theft, cyberterrorism, incitement of religious hatred via social or electronic media, and hacking. However, according to Amnesty International, this new legislation proved to be more draconian[63] and has since been used as a political instrument to suppress dissent, targeting journalists, academics, activists, politicians, students, and other dissenting voices.[64] Under the repressive law, writer Mushtaq Ahmed died in custody, and cartoonist Ahmed Kabir Kishore suffered severe torture in jail.[65] Eventually, in the face of immense pressure, both from international condemnation and domestic protests[66], this law, too, was scrapped, only to be substituted by another oppressive law—the Cyber Security Act of 2023.[67]

61 Ali Riaz, (n 5) 6–7.

62 For a detailed report, see Human Rights Watch, (n 5) 32–63, 70–89.

63 *Bangladesh: Muzzling Dissent Online* (n 5) 2.

64 For a detailed analysis, see Riaz, (n 5) 13-30; OHCHR, *Technical Note to the Government of Bangladesh on Review of the Digital Security Act* (Technical Note, June 2022) 1–11 https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf.

65 *Amnesty International, Bangladesh: Cartoonist Tortured, Writer Dies in Jail* (Letter to Prime Minister Sheikh Hasina, 2021) https://www.amnesty.org/en/wp-content/uploads/2021/05/ASA1338002021ENGLISH.pdf; Human Rights Watch, *Bangladesh: Writer Dies After 9 Months in Custody – Held in Pretrial Detention After Criticizing Government* (26 February 2021) https://www.hrw.org/news/2021/02/26/bangladesh-writer-dies-after-9-months-custody.

Besides curbing the right to the freedom of expression of its citizens, the Bangladesh Government has a notorious track record of engaging in surveillance activities violating fundamental human rights, particularly the right to privacy. In the aftermath of blogger killings from 2013 to 2015 and the 2016 Holey Artisan attack in Dhaka, under the pretext of countering violent extremism and terrorism, the government of Bangladesh conducted arbitrary monitoring and wiretapping of suspected citizens by collecting massive data which included bank information, business records, cell phone activity, body and bag scans, facial recognition via CCTV, and cross-border movement tracking.[68]

According to the Tech Global Institute, from 2015 to 2025, the Bangladesh government procured at least 160 surveillance technologies and spyware at an estimated cost of USD 184.5 million.[69] These tools include audio surveillance devices such as laser microphones; spyware like Pegasus, Predator, WiSpear, and FinFisher; AI-powered video surveillance systems with facial recognition; mobile and Wi-Fi interceptors such as IMSI catchers; and software capable of full device access. Other technologies reportedly acquired include geolocation trackers, forensic extraction tools such as Cellebrite UFED, deep packet inspection systems for monitoring internet traffic, and jamming devices used to

66 See OHCHR, *Bangladesh: Bachelet Urges Review of Digital Security Act Following Death in Custody of Writer* (Statement and Speech, 1 March 2021) https://www.ohchr.org/en/statements-and-speeches/2021/03/bangladesh-bachelet-urges-review-digital-security-act-following (The former UN High Commissioner for Human Rights, Michelle Bachelet, expressed serious concern for human rights violations under the DSA, and urged the Government "to suspend the application of the Digital Security Act and conduct a review of its provisions to bring them in line with the requirements of international human rights law."). Similar concerns have been expressed by Volker Türk, the current UN High Commissioner for Human Rights, condemning the grave human rights violations under the Act, and calling for an immediate suspension of its application, see OHCHR, *Bangladesh: Türk Urges Immediate Suspension of Digital Security Act as Media Crackdown Continues* (Press Release, 31 March 2023) https://www.ohchr.org/en/press-releases/2023/03/bangladesh-turk-urges-immediate-suspension-digital-security-act-media?ref=netra.news. See also, *Faisal Mahmud, Anger in Bangladesh over Dissident Writer's Death in Prison* (26 February 2021) Al Jazeera https://www.aljazeera.com/news/2021/2/26/anger-in-bangladesh-over-prominent-writers-death-in-prison; *Protests over Prison Death of Bangladeshi Writer* (27 February 2021) DW https://www.dw.com/en/bangladesh-protests-erupt-over-writers-death-in-prison/a-56723169; *Faisal Mahmud, Bangladesh to Tone Down 'Draconian' Digital Security Law* (7 August 2023) Al Jazeera https://www.aljazeera.com/news/2023/8/7/bangladesh-to-tone-down-draconian-digital-security-law; I*nternational Pressure Builds on Bangladesh Government to Suspend Digital Security Act* (Blog Post, 31 March 2023) Netra News https://netra.news/2023/international-pressure-builds-on-bangladesh-government-to-suspend-digital-security-act/.

67 For detailed analysis, see Nusmila Lohani, *DSA Has a New Name: CSA* (15 September 2023) The Business Standard https://www.tbsnews.net/features/panorama/dsa-has-new-name-csa-700830; Ahamed Ullah *et al, Cyber Security Act Will Not Stop Criminalising Freedom of Expression* (13 August 2023) *The Daily Star* https://www.thedailystar.net/opinion/views/news/cyber-security-act-will-not-stop-criminalising-freedom-expression-3393326; Zillur Rahman, *The New CSA: A Draconian Law Made More 'Efficient'* (24 August 2023) The Daily Star https://www.thedailystar.net/opinion/views/news/the-new-csa-draconian-law-made-more-efficient-340115; Nowzin Khan, *From DSA to CSA: The Same Two Bottles of Agony* (26 August 2023) *The Daily Star* https://www.thedailystar.net/opinion/views/news/dsa-csa-the-same-two-bottles-agony-3403566; Repackaging Repression (n 5).

68 Sabhanaz Rashid Diya, *Beyond the Shadows: Reforming Surveillance Practices in Bangladesh* (6 October 2024) *The Daily Star* https://thegreatwave.thedailystar.net/news/beyond-the-shadows-reforming-surveillance-practices-in-bangladesh.

69 Tech Global Institute, *The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh 23* (Report, August 2025) https://techglobalinstitute.com/wp-content/uploads/2025/08/TGI-Cyber-Surveillance-Practices-in-Bangladesh-F.pdf.

disrupt wireless communications—sourced from at least thirty companies providing surveillance and hacking services.[70] These companies are from countries including the U.S., U.K., France, Germany, Switzerland, Italy, Lithuania, Russia, Israel, India, Turkey, China, Cyprus, and Canada.[71]

The unchecked surveillance activities and monitoring have been facilitated by Section 97A of the Bangladesh Telecommunication Regulation Act 2001. This provision allows the government to authorize intelligence agencies, national security agencies, investigative agencies, and law enforcement officers to intercept, record, or collect information from any telecommunications service user under the pretext of national security or public order.[72] It provides blanket authority to the National Telecommunications Monitoring Centre (NTMC), Directorate General of Forces Intelligence (DGFI), National Security Intelligence (NSI), Rapid Action Battalion (RAB), or any empowered law enforcement or investigative unit, without any procedural safeguards or limitations. Telecommunication service providers are legally obligated to comply with government directives to assist in interception or data collection. Noncompliance could result in penalties or cancellation of licenses, creating pressure to cooperate, even if actions are unethical or lack judicial backing.[73]

There is no requirement to define specific threats or obtain a court order. Instead, surveillance can be carried out through executive discretion from the Ministry of Home Affairs and approved by the Minister or State Minister. This lack of checks and balances increases the risk of abuse of surveillance powers. Additionally, terms such as "national security" and "public order" are not clearly defined, allowing for subjective interpretation.

These laws—the Information and Communication Technology (ICT) Act of 2006, the Digital Security Act (DSA) of 2018, the Cyber Security Act of 2023, and the Bangladesh Telecommunication Regulation Act of 2001—share a common pattern of law drafting—characterized by vague provisions, overly broad and arbitrary powers of the Government, insufficient safeguards and disproportionate restriction on fundamental human rights.[74]

The recent Fact-Finding Report on Human Rights Violations and Abuses Related to the Protests of July and August 2024 in Bangladesh, published by the OHCHR, finds that surveillance through digital laws has been weaponised to systematically suppress democratic protests and stifle dissenting voices.[75] The report reveals serious human rights violations, including extrajudicial killings, the arbitrary use of force

70 ibid.

71 ibid 64; Surveillance Watch, Country Profile: Bangladesh https://www.surveillancewatch.io/?country=Bangladesh. See also Al Jazeera Investigative Unit, 'Bangladesh Bought Mass Spying Equipment from Israeli Company', *Al Jazeera* (Online, 2 February 2021) https://www.aljazeera.com/news/2021/2/2/bangladesh-bought-surveillance-equipment-from-israeli-company; Oded Yaron and Zulkarnain Saer Khan, 'Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record', *Haaretz* (Online, 10 January 2023) https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000.

72 *Bangladesh Telecommunication Regulation Act 2001* (Bangladesh), s 97A ('*BRTA*').

73 ibid s 46.

74 See Article 19, (n 5) 4–19; OHCHR, *Technical Note* (n 57); *Repackaging Repression* (n 5) 17–26; Shahzeb Mahmood and Sabhanaz Rashid Diya, *A New Digital Frontier: A Blueprint for Reforms towards Rights-Respecting Information and Technology Laws in Bangladesh* (White Paper, Tech Global Institute, 2024) 59 https://techglobalinstitute.com/wp-content/uploads/2024/12/Whitepaper-A-New-Digital-Frontier-Bangladesh.pdf.

75 OHCHR, *Fact-Finding Report on Human Rights Violations and Abuses Related to the Protests of July and August 2024 in Bangladesh* (United Nations Report, 12 February 2025) i–ii, 7–8, 45, 46, 64, 72–3 https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/ohchr-fftb-hr-violations-bd.pdf.

against protesters, widespread arbitrary arrests and detentions, as well as torture and other forms of ill-treatment committed by the Directorate-General of Armed Forces Intelligence (DGFI), National Security Intelligence (NSI), Rapid Action Battalion (RAB) and the National Telecommunication Monitoring Centre (NTMC) – and the specialized branches of the Police – Detective Branch, Special Branch and Counter Terrorism and Transnational Crime unit (CTTC).[76]

5.2 National Security Exemptions, Related Overbroad Provisions, and Their Possible Ramifications

A closer inspection of the Draft Personal Data Protection Ordinance of 2025 finds the same arbitrary and overbroad features, which raise grave concerns for the privacy rights of the citizens. One of the core objectives of the draft Ordinance is to protect the privacy rights of an individual's personal data.[77] Even personal data has been recognized as a personal right of a data subject.[78] However, the draft notably fails to explicitly reference the right to privacy through a dedicated section or provision and make it a foundational and substantive right under the Ordinance. It adopts a functionalist and administrative approach that treats privacy as a policy objective rather than a fundamental right.[79] By omitting any explicit reference to the constitutional right to privacy, the draft Ordinance reduces data protection to a regulatory issue, rather than affirming it as a safeguard of individual autonomy and dignity. This signals a preference for a control-based or compliance-driven framework, which weakens the normative emphasis on protecting individuals' rights. The omission of an explicit reference to the right to privacy in the 2025 draft Ordinance is not a mere drafting choice—it likely reflects a deliberate de-prioritization of individual rights in favor of state control. This weakens the legal foundation of the data protection regime, raises serious concerns about surveillance and executive overreach, and places Bangladesh at odds with constitutional obligations and international data protection standards.

Particularly under Sections 5(6)(b) and 48, the draft Ordinance has granted vast power to the Government, enabling it to access, store, and monitor an individual's personal data without accountability, which may result in serious privacy rights violations. Section 5(6)(b) allows data fiduciaries to process personal data "in such manner as may be prescribed by regulations" where the processing is considered necessary for national security interests. Thus, under regulations made by the Authority,[80] which may not stipulate the requirement of knowledge or consent of the data subjects, any personal data, potentially including sensitive personal data,[81] can be processed without meaningful safeguards or oversight as the provision is not qualified by any requirement of necessity, proportionality,

76 ibid.

77 *DPDPO* (n 19) Preamble, s 19 (Explanation clause).

78 ibid Preamble.

79 See ibid s 29(b), (c), (h), which provides that the Authority shall, in addition to its responsibilities under the *Data Governance and Interoperability Authority Ordinance 2025*, (b) promote the protection and observance of the right to privacy and the protection of personal data; (c) monitor, investigate, and report on the observance of the right to privacy and the protection of personal data; and (h) establish and maintain a personal data protection and privacy register.

80 See ibid s 54 (This provision empowers the Authority to "make regulations on the subject matters as designed in the provisions of this Ordinance but do not fall within the purview of rules.").

81 ibid s 2(t) defines "sensitive personal data" to include genetic and biometric data, information on ethnic or racial identity, political or religious beliefs, trade union membership, health and sexual life, alleged criminal offenses, real-time location linked to personal identification, and other critical personally identifiable information.

or judicial authorization. Sensitive personal data includes biometric information, ethnicity, health, political opinions, religious beliefs, associations, sexual life, and criminal records; real-time location data; and critical personally identifiable information (PII), such as phone numbers, IP addresses, and bank account details. It also encompasses any other categories of personal data that may be prescribed by rules. Since the Government holds the authority to promulgate such rules, it may expand the scope of sensitive personal data to include additional categories—such as phone call records, private messages, social media activity, emails, and passwords—through subordinate legislation.

The absence of substantive safeguards against such arbitrary encroachment upon personal data means that individuals are left without remedies or recourse in cases of rights violations. This could lead to systemic misuse of personal and sensitive data, especially for profiling, secret surveillance, and political targeting under the guise of national security.

Furthermore, while Section 8 provides additional conditions for processing sensitive personal data, including health, ethnicity, legal, and employment data, the national security exemption indirectly undercuts those conditions. Since the government or its agencies could invoke Section 5(6)(b) to process even sensitive personal data without consent or judicial oversight, the layered protections offered in Section 8 risk becoming meaningless in practice.

Among all, Section 48 is the most overarching provision, which has vested power in the Government to instruct the Authority to comply with its whimsical directives on national security grounds. This means the Authority is unable to act independently or make autonomous judgments, as the Government retains full control over regulatory functions. Potentially, under this single provision, the Government can override any rights and any safeguards provided to the data subject. Although the Ordinance includes a catalogue of data subject rights, which provides for access (Section 11), correction (Section 12), withdrawal of consent (Section 13), erasure (Section 15), and prevention of processing (Section 16), these rights are practically inoperable when overriding national security exemption is invoked under Section 48.

Section 15(2) allows data fiduciaries to refuse erasure on vague grounds like "public interest data" or "archival purposes," terms that remain undefined and prone to broad interpretation, even national security interests can fit in these broad grounds. Moreover, the classification mechanism under Section 10, allows the Authority to categorize data fiduciaries based on their perceived impact on national security, sovereignty, democracy, or public order and Section 34 permits classification of certain categories of personal data, such as those relating to national security, defense, and public safety, which can be classified as "Confidential and Restricted" and mandates data localization. While data localization may be justified on security grounds, the classification mechanism itself is opaque, as on its face this may appear to be a regulatory risk-based model, in the current political context of Bangladesh, marked by democratic backsliding and executive overreach, this mechanism is concerning as it could be used to selectively target NGOs, civil society actors, activists or political opponents by subjecting them to enhanced surveillance or data control obligations.

Since there is no independent supervisory or regulatory authority to oversee citizens' personal data protection, the Government will have unlimited access to a person's personal data to monitor and conduct secret surveillance. The absence of an independent authority creates opportunities for the

Government to act capriciously and pursue questionable agendas. Even no judicial oversight or judicial review system has been ensured to oversee the surveillance initiatives. The Authority will not require any court order to carry out surveillance following the government's directive. These provisions do not set any procedural standards for necessity and proportionality when intruding on a person's data, making them arbitrary and leaving room for excessive and abusive enforcement. In such a framework, executive claims of national security become unchallengeable, turning the Authority into an enabler rather than a check on data abuse.

Additionally, the Draft Ordinance nowhere defines "security of the State." A clear definition of "security of the State" can help determine the boundaries of state power, but without a specific definition, national security can be subjectively interpreted very broadly by the government and security agencies. Furthermore, it fails to specify what types of personal data or under what circumstances an individual's personal data may be subject to scrutiny for national security interests and for how long these data may be retained. This lack of clarity will allow unwarranted interception and surveillance of personal data without any legitimate or imminent threat to national security. In the absence of a precise determination of the types of personal data that may be subject to national security interests and the circumstances under which such data can be accessed, virtually any personal data may be collected, stored, and examined. Individuals lack the right to be notified about data processing on national security grounds. However, storing personal data of an individual's private life by a public authority, regardless of how the data is obtained and whether such data is subsequently used, is an interference with the right to respect for the data subject's private life.[82] Hence, alarmingly, the lack of a specified data retention period for processing data in national security interests will further enable the state to carry out targeted or mass secret surveillance indefinitely. Even the data retention principle outlined in the draft Ordinance conflicts with global best practices. According to the draft, an individual's personal data can be permanently destroyed only if "it is no longer permitted to be retained [by the Authority or the Government]."[83] Contrarily, the GDPR adopts a 'storage limitation principle,' which mandates that personal data must be erased when they are no longer necessary for the original, lawful collection purposes.[84]

While the overall arbitrary application of digital laws in the past has instilled a profound fear that this draft Ordinance will inevitably be used for similar purposes, this fear is primarily fueled by Section 97A of the Bangladesh Telecommunication Regulation Act of 2001[85] —an existing national security exemption that has been widely abused. This section has excessively empowered the government to illicitly intercept, record, and examine citizens' phone calls and private messages, mostly for political ends.

The draft Ordinance introduces equally

82 See *Amann v Switzerland* [GC] (European Court of Human Rights, Application No 27798/95, 16 February 2000) [69]; *Rotaru v Romania* [GC] (European Court of Human Rights, Application No 28341/95, 4 May 2000) [46]; *S and Marper v United Kingdom* [GC] (European Court of Human Rights, Application Nos 30562/04 and 30566/04, 4 December 2008) [67]; *M K v France* (European Court of Human Rights, Application No 19522/09, 18 April 2013) [29]; *Aycaguer v France* (European Court of Human Rights, Application No 8806/12, 22 June 2017) [33].

83 *DPDPO* (n 19) s 4(c).

84 See Matthias Enzmann, Annika Selzer and Dominik Spychalski, 'Practitioner's Corner – Data Erasure under the GDPR – Steps towards Compliance' (2019) 5(3) *European Data Protection Law Review* 416, 416.

85 *BRTA* (n 72).

concerning national security exemptions within Sections 5(6)(b) and 48. The convergence of these provisions with the notorious Section 97A creates a truly deadly combination. This potent legal framework would empower the Government and security agencies to collect and access personal data without adequate oversight and accountability, paving the way for the pervasive misuse of national security exemptions in both laws to justify institutionalized arbitrary surveillance, thereby fundamentally eroding the privacy and data protection rights under the guise of national security.

Notably, in 2019, the High Court Division of Bangladesh observed that government agencies accessing customer data without due process or user notification violates the right to privacy protected by Article 43 of the Constitution of Bangladesh.[86] Without judicial supervision and necessary checks on the executive power, the government wields excessive, unchecked power to conduct surveillance without consent, restrict a person's access to data, and process data in secrecy.

Additionally, Section 30 granted the Data Protection Authority unchecked discretionary powers without defining clear limits, checks, or procedural safeguards. It empowers the Authority to "take any measures and exercise any powers necessary" for carrying out its functions, including access to data for inquiry or investigation. Section 31 allows the Authority to issue a binding standard operating procedure that effectively acts as secondary legislation and creates a scope for politically motivated rule-making in critical areas of data governance. Under Section 38, a data subject is permitted to file complaints when their rights have been infringed upon to the Authority, rather than before any court. Moreover, although Section 47 permits an appeal for any aggrieved person, that appeal must also go to an Appellate Authority established by the Government, not a court. The ultimate rule-making power lies with the Government, as it can make rules by notification to "carry out the purposes of this Ordinance."[87]

As a result, these provisions concentrate excessive power in the executive branch by delegating both rule-making and adjudicatory authority to it, lacking robust parliamentary oversight or judicial review mechanisms. The government ultimately retains complete control over the Data Protection Authority and the Appellate Authority—appointing members, setting service terms, and issuing binding directions, which undermines their independence and denies individuals access to an impartial adjudicatory body, despite the government's role as a major data fiduciary. Considering the national security provisions and other overly broad provisions, the Ordinance lacks the necessary 'quality of law' as it grants the executive authority excessive discretionary power without clearly defining the scope and manner of its application.[88]

According to the OCHR, the State has a duty to ensure that "any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances

86 *The State and Ors v Oli and Ors* (2019) 73 DLR (2021) 514, [64].

87 *DPDPO* (n 19) s 53.

88 See *Right to Privacy Report* (n 31) [29]; *Roman Zakharov* (n 47) [302]–[304]. (The Court held that without proper judicial authorization of surveillance, it renders arbitrary and abusive surveillance practices which are incapable of keeping the "interference" to what is "necessary in a democratic society".).

in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse."[89] While the draft Ordinance is publicly accessible, it utterly fails to meet the remaining requirements.

Therefore, with its arbitrary provisions, the draft Ordinance risks reinforcing authoritarian governance in Bangladesh. Its broad national security exemptions could grant the government limitless surveillance powers, severely infringing on citizens' privacy and data protection rights without accountability. As Bangladesh has a struggling democracy with authoritarian tendencies and power centralization, it remains possible to turn the draft Ordinance into law and exploit it for a firm, undemocratic consolidation of power, which is highly undesirable. The Draft Personal Data Protection Ordinance should be revised to include sufficient guarantees, especially against overly broad national security exemptions, and it must incorporate standards of necessity and proportionality. This is crucial to uphold democratic values and to ensure that the right to privacy is protected as a cornerstone of the freedoms essential to democracy, which include freedom of expression, thought, assembly, and dissent. As the High Court Division affirmed in 2016, "The right to privacy is an essential foundation of the freedom of dissent. So, this right cannot be undermined in the name of surveillance."[90]

6. CONCLUSION

The article finds that paradoxically, the law titled the *Personal Data Protection Ordinance, 2025*—which purports to protect personal data—deliberately by design omits any explicit and direct reference to the right to privacy, which is enshrined in the Constitution and the ICCPR, and is of utmost significance for the personal data protection of individuals. The draft Ordinance, however, prioritizes regulatory mechanisms over the protection of citizens' data and privacy rights.

Undoubtedly, national security is fundamental to any state's survival, for which the state indeed enjoys a wide margin of appreciation regarding national security exemptions in any law. However, this wide discretion cannot be exercised arbitrarily or exploited for political advantage. In reviewing the draft Ordinance's national security exemption provisions and other related provisions, this article identifies a critical omission: the absence of core safeguards against abuse, particularly the principles of necessity and proportionality. Moreover, these provisions are framed so broadly that they may enable the Government to conduct arbitrary mass surveillance, significantly infringing on individuals' right to privacy. Accordingly, the Government's overreach in surveillance capabilities for securing national security interests without adequate protections for citizens' data and privacy calls into question whether the proposed Ordinance meets the 'quality of law' standard.

Drawing on global best practices and relevant jurisprudence, the article has demonstrated how the principles of necessity and proportionality are central to any lawful limitation on the right to privacy. Given Bangladesh's troubling record of surveillance and the abuse of digital laws to suppress dissent and target political opposition, the current draft of the Ordinance poses serious worries. In light of these findings, this article recommends that the draft should be revised

89 *Right to Privacy Report* (n 31) [28].

90 *Aynunnahar Siddiqua and Ors v Government of Bangladesh and Ors* LEX/BDHC/0175/2016, [2].

to explicitly incorporate these standards for accessing and processing personal data in the interests of national security, ensuring that data fiduciaries, the National Data Governance and Interoperability Authority, security agencies and the Government must strictly adhere to these principles when conducting their data processing activities. For surveillance on the grounds of national security to be justified and nonarbitrary, it must be strictly necessary to advance democracy in the country, and strictly proportionate in limiting privacy while protecting national security in the least intrusive way.

In line with the best practices, the Ordinance should be amended to provide that any exemption from, restriction on, or derogation of a data subject's rights under the Ordinance on grounds of national security shall only be permitted where such measures respect the essence of fundamental rights and freedoms, and are both necessary and proportionate in a democratic society.[91]

Additionally, surveillance for securing sovereignty and integrity must be subject to robust judicial oversight so that the Authority cannot act arbitrarily and conduct secret surveillance activities on individuals without reasonable grounds and a court order.[92] Judicial control is essential to ensure that any surveillance activity conducted on national security grounds conforms to the principles of necessity and proportionality. Without such oversight, a regime of secret surveillance—undertaken in the name of national security—risks subverting or even dismantling democratic institutions under the guise of protecting them.[93]

The vague and undefined terms "sovereignty," "integrity," and "security of the State" must be clearly defined within the Ordinance. A precise definition of these terms can limit the government from arbitrarily invoking national security to bypass data protection and privacy rights obligations. Moreover, a well-defined concept of national security, along with the types of personal data that fall under its scope, and strict limits on the data retention period, can aid in striking a balance between state security interests and individual privacy rights. This transparency can ensure that security measures are proportionate and do not infringe on fundamental rights more than necessary. It will also help individuals to understand when their data may be accessed or restricted by the state.

Overall, the Ordinance currently grants unchecked authority to access and process a wide array of sensitive personal data, such as biometric data, health information, political opinions, details about sexual life, and real-time location, without adequate and effective safeguards. This intrusion undermines the individual's right to privacy. In turn, this massive interference with personal data would also adversely affect other

91 See *GDPR* (n 15) art 23; *PDPA* (n 18) s 40.

92 *Klass v Germany* (Application No 5029/71), European Court of Human Rights, 6 September 1978, [54]–[57], [67], [75] (The Court acknowledged that judicial oversight of surveillance is generally preferable. However, it determined that the system in place, which involved a non-judicial supervisory control carried out by a Parliamentary Board and a Commission appointed by that Board, provided adequate safeguards against potential misuse of surveillance powers.); *Szabó* (n 44) [73]–[77] (Emphasizing its preference for judicial oversight, the Court stated that surveillance measures should primarily fall under judicial control, making any substitute solutions exceptional and subject to close scrutiny.); *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (C-311/18) [2020] ECLI:EU:C:2020:559, [65], [187]–[194] (The court struck down EU-US data sharing because US surveillance laws lacked adequate judicial oversight and protection.).

93 See *Roman Zakharov* (n 47) [232]; *Szabó* (n 44) [57].

fundamental rights, such as the right to freedom of expression, thought, religion, assembly, and association, as they are closely linked. Without judicial control, oversight, and adherence to principles of necessity and proportionality, national security exemptions and other overly broad provisions that enable excessive accumulation of rule-making and adjudicatory power become dangerous loopholes that can be exploited for authoritarian ends. As a result, the draft Ordinance carries the risk of potentially becoming another draconian law, as it appears to contravene the core spirit of the July Uprising of 2024, which aimed to reinstate democratic governance, uphold the rule of law, and protect human rights within Bangladesh. As Bangladesh is a ratifier of the ICCPR, per the Human Rights Committee's interpretation of article 17, it is duty-bound to ensure "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."[94]

94 See *Toonan v Australia*, UN Human Rights Committee, Communication No 488/1992, UN Doc CCPR/C/50/D/488/1992 (31 March 1994) [8.3]; *Van Hulst v Netherlands*, UN Human Rights Committee, Communication No 903/1999, UN Doc CCPR/C/82/D/903/1999 (15 November 2004) [7.3]; *M.G. v Germany,* UN Human Rights Committee, Communication No 1482/2006, UN Doc CCPR/C/93/D/1482/2006 (16 July 2008) [10.1]–[10.2].

LIABILITY OF TELCOS FOR HUMAN RIGHTS VIOLATIONS

Case Study of Internet Shutdowns in Bangladesh

Nazifa Muniyat Quader

Abstract

This paper examines the legal implications of state-mandated internet shutdowns and the role of telecommunication companies (telcos) navigating conflicting domestic laws and international human rights obligations. Analyzing regional precedents and the July 2024 internet shutdown in Bangladesh, it evaluates telcos' potential criminal liability for enabling state-backed atrocities. The study highlights the inadequacy of current international frameworks, such as the ICJ and *erga omnes* obligations to hold authoritarian states accountable or protect resisting telcos. Ultimately, it argues that absent robust legal mechanisms, telcos remain vulnerable to weaponized digital repression, frequently operating as involuntary facilitators of severe human rights violations.

Keywords: *Telecommunication Companies, Internet Shutdown, Freedom of Expression, Criminal Liability.*

1. INTRODUCTION AND BACKGROUND

Since 2019, Bangladesh has faced around 10 cases of internet shutdowns, with at least three of those blackouts being partial service block and three others being nationwide blockage, while the rest were regional in nature.[1] Internet blackouts, which result in information blackouts, have often been used as a tool for conducting state-backed mass atrocities.[2] Further, internet blackouts have long been used as a tool for suppressing dissenting opinions and legitimate protests against governments.[3] For example, in 2018, a nationwide slowdown of mobile networks was executed in response to a road safety protest.[4] Mobile network operator companies, or otherwise known as telecom companies (hereinafter referred to as "Telcos") are among the key actors at the crossroads of internet blackouts.

Section 46 of the Information and Communication Technology Act, 2006 ("ICT Act") in Bangladesh empowers the government to block the dissemination of any information through any computer resource. This section provides, "*If the regulator is satisfied that, in the interest of Bangladesh's sovereignty, integrity, security, friendly relations with foreign states, public order and safety, or for the prevention of incitement to commit any offence punishable under this Act, it is appropriate and necessary to issue a directive, then they may, by written order stating reasons, instruct any government law enforcement agency to block the dissemination of any information through any computer resource.*" Section 97A of Bangladesh Telecommunication Act, 2001 ("BTRC Act") states more directly, "*Notwithstanding anything contained in this or any other law, in the interest of national security or public order, the government may, from time to time and for a specified period, authorize any officer of an intelligence agency, national security agency, investigative agency, or law enforcement authority to intercept, record, or collect information related to any message or communication transmitted by a telecommunications service user, the government may also direct the telecommunications service provider to fully cooperate in such activities, and the operato*r shall be obliged to comply with such directives." Thus, in accordance with these provisions, where the information is such that it ought to be divulged in the public interest, the government may require blocking, as well as disclosure of such information, therefore restricting the right to freedom of expression and privacy. Information relating to anti-national activities, breaches of the law or statutory duty or fraud may fall under this category. The government may also restrict freedom of expression on grounds of national interest. A denial of compliance with such government order takes a direct effect on the license of that Telco under Section 46 of the BTRC Act, rendering it susceptible to being unable to conduct business in Bangladesh. Often, the definition of public interest is broadly interpreted, leading to categorical internet shutdowns and dissemination of information even without valid grounds of public interest. Internet blackouts are weaponized to prevent

1 "Global Internet Shutdowns." *Internet Society Pulse*, https://pulse.internetsociety.org/shutdowns. Accessed 28 Mar. 2025.

2 "Internet Shutdowns Shroud and Facilitate Brutality of Myanmar Junta's Airstrike in Hpakant Township." Access Now, 27 Oct. 2025, https://www.accessnow.org/press-release/myanmar-internet-shutdown-hpakant/.

3 "Internet Blackouts in Bangladesh: A Breach of Fundamental and International Human Rights" Youth Policy Forum, 4 Aug. 2024, https://ypfbd.org/internet-blackout-in-bd/.

4 L'Agence France-Presse. "Unrest in Bangladesh as Student Road Safety Protests Turn Violent."; The Guardian, 5 Aug. 2018. The Guardian, https://www.theguardian.com/world/2018/aug/05/bangladesh-pm-urges-teen-protesters-to-go-home-amid-violence.

the citizens from assembling and organizing, when state-backed mass atrocities are committed.[5] In these situations, multinational companies having certain bargaining powers are often expected to push back against unreasonable orders, when compliance with such orders may lead to massive implications for human rights.[6] This paper attempts to foresee the legal compliance issues and implications that these companies might face in situations where they resist state-mandated internet shutdowns instead of caving in. It analyzes the legal implications of pushbacks against arbitrary internet shutdowns, and implications in cases of mass human right contempt of peremptory norms.

2. THEORETICAL CONSTRUCTION

2.1. What Constitutes Human Rights Violation During an Internet Shutdown?

The right to uninterrupted internet access is not recognized as a standalone human right. However, violation of this right directly prejudices people's right to freedom of expression, which is guaranteed as a fundamental human right in the Universal Declaration of Human Rights[7] (hereinafter. 'UDHR'), and the International Covenant on Civil and Political Rights[8] (hereinafter 'ICCPR'). Article 19 of the UDHR states that "*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas* through any media and regardless of frontiers". Article 19 of ICCPR also guarantees the right to freedom of expression, including the freedom to seek, receive, and impart information. There are other regional conventions such as European Convention on Human Rights (ECHR), African Charter on Human and Peoples' Rights and American Convention on Human Rights that protects Freedom of Expression and Right to Information without interference from public authorities;[9] affirms right to receive and disseminate information;[10] and prohibits prior censorship[11] respectively – leading to strong legislative presence. Though the international instruments are binding upon all their signatories, the mechanism for implementation of the rights enshrined in those varies across jurisdictions. For example, implementation of these rights is likely to be easier in monist states, where the international law applies directly. Conversely, states requiring a separate legislative act to transform an international rule into national law may face additional hurdles and delays.

Alongside the right of freedom of expression reflected in international instruments, it is also a constitutionally guaranteed right in Bangladesh,[12] as well as in India.[13] In

5 Mahmudul Hasan, 'What You Need to Know about Internet Crackdown in Bangladesh' *The Daily Star*, (Dhaka, 13 August 2024) https://www.thedailystar.net/business/news/what-you-need-know-about-internet-crackdown-bangladesh-367634

6 David Sullivan, 'Five Ways Telecommunications Companies Can Fight Internet Shutdowns', *Lawfare*, (Washington, D.C., 23 August 2020) https://www.lawfaremedia.org/article/five-ways-telecommunications-companies-can-fight-internet-shutdowns.

7 Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR) art 19.

8 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 19.

9 European Convention on Human Rights a 10.

10 African Charter on Human and Peoples' Rights a 9.

11 American Convention on Human Rights a 13.

12 *Constitution of the People's Republic of Bangladesh*, art 39.

13 *Constitution of India*, art 19.

recognition of the impact of internet shutdowns on human rights, the Kerala High Court of India has recognized in *Faheema Shirin v. State* of Kerala, that internet shutdowns violate constitutional rights, and any restriction upon these rights may be imposed only in accordance with the constitutional norm of reasonable restriction.[14]

While the right of freedom of expression is indeed not absolute, and is subject to reasonable restrictions, any such restriction must strictly comply with the legal framework, for example the one provided in Article 19(3) of ICCPR. The general comment to this Article provides that, for a restriction on this right to be legal, the scope of restriction must be prescribed by law, it must be imposed only to pursue a legitimate objective, and must be necessary and proportionate to achieve the aim of the restriction.[15]

2.2 What Do We Mean by Liability of Telcos for Human Rights Violation?

During Internet shutdowns, human right violations mainly take place in two-folds. The first being restrictions on freedom of expression, freedom of press, and the right to information. These restrictions may be justified if the necessity of imposing such restrictions far outweighs the consequent harm of limiting these fundamental freedoms. Secondly, the censorship and control of information by an Authoritarian government to carry out mass surveillance, suppress dissent, and maintain control, is a further, and immense, violation of human rights that can occur during Internet blackouts. Often, such governments weaponize Internet blackouts to order law enforcement agencies to apply excessive force, subject individuals to enforced disappearance, and take people into custody – essentially using blackouts as a tool to violate the right to life and personal liberty, and leaving no room for dissent. In circumstances where such human rights violations occur, Telcos are directed by the government to shut down the Internet, making them a direct stakeholder in Internet shutdowns.

The judicial history of Pakistan is particularly relevant in this context, notably the legal arguments surrounding whether "mere apprehensions" of an untoward incident justify the suspension of cellular services and internet shutdowns. This issue was prominently addressed in the case of CM Pak Limited v. Pakistan Telecommunication Authority.[16] The dispute arose when CM Pak Limited, a licensed mobile service provider, filed a petition challenging the Pakistan Telecommunication Authority's (PTA) power to suspend services based on mere apprehensions, arguing it was a violation of the Constitution and a breach of customer obligations. Ruling on the matter in 2018, the Islamabad High Court stated, "In the instant case, the appellant Company has impugned the orders/directives of the Authority regarding the blocking or suspension of mobile cellular services on the basis of mere apprehensions relating to avoiding an untoward incident. Such orders/directives were definitely in violation of the express provisions of the Act of 1996, particularly section 54(3)." The Court further noted, "The Federal Government or the Authority are, therefore, not vested with the power and jurisdiction to suspend or cause the suspension of mobile cellular services or operations on the ground of national security except as provided under section 54(3)."[17]

14 AIR 2020 Ker 35.

15 UN Human Rights Committee, '*General Comment No 34: Article 19: Freedoms of Opinion and Expression*' (12 September 2011) UN Doc CCPR/C/GC/34.

16 *CM Pak Limited v Pakistan Telecommunication Authority* (Islamabad High Court, 26 February 2018) FAO 42 of 2016.

17 ibid.

However, it is important to note that this stance was ultimately reversed in 2020, when the Supreme Court of Pakistan set aside the High Court's judgment and upheld the government's authority to execute such suspensions.[18]

3. CASE STUDY: INTERNET SHUTDOWNS IN BANGLADESH

3.1 Examining Cases of Internet Shutdowns and human rights violations

Existing legal frameworks in Bangladesh currently empower the Bangladesh Telecommunication Regulatory Commission (hereinafter "BTRC" or 'the Commission") to exert control and authority over telcos; the Commission can act as a henchman for an Authoritarian regime, and it does not shy away from acting as such from time to time. As the government mandated licencing Authority, BTRC often coerces telcos to share subscriber data, leveraging its unilateral authority to grant and withhold licenses according to its licensing framework.[19] The BTRC Act, 2001 prohibits the establishment, operation, or use of telecommunication systems including radio apparatus and providing telecommunication services in Bangladesh without a license provided by the BTRC, under Sections 36 and 55. These provisions empower BTRC to have a hold over the licensing of the telcos, on behalf of the government and its interests. Though the Regulatory and Licensing Guidelines for Cellular Mobile Services in Bangladesh mandate the license operations to act in accordance with safeguards enshrined in the principles of transparency, fairness, non-discrimination,[20] In reality, the decisions taken are often imposed and lack transparency, and Telcos are not provided the opportunity to be heard. For example, following the death of Abrar Fahad in 2019, a BUET-based sub-domain was acting as a 'one-stop online reporting system.' It listed over 150 complaints anonymously made by current and former students of the Bangladesh University of Engineering and Technology (BUET), mostly against the Bangladesh Chhatra League, the student body of the ruling party at the time. With 72 complains being listed within two days of the Abrar Fahad murder, BTRC ordered all IIG and ISP operators in the country to block the domain. The email issuing the order did not provide any reasons behind such a decision.[21] The stakeholders of the sub-domain were not given a chance to defend themselves against the order. This instance is but one example highlighting how the BTRC had often acted arbitrarily, and even lacked the basic decency of hearing out both parties. This indicates that the Commission was under the impression that it was exempt from accountability.

3.2 Assessing Role of Telcos During Human Rights Violation

As corporate representatives, and a direct stakeholder in Internet shutdowns, telcos are

18 *Pakistan Telecommunication Authority v CM Pak Limited* (Supreme Court of Pakistan, 22 April 2020) Civil Appeals 977 and 978 of 2018.

19 Tech Global Institute, *The Digital Police State: Cyber Surveillance Practices in Bangladesh* (Tech Global Institute 2025) 17.

20 Bangladesh Telecommunication Regulatory Commission, *Regulatory and Licensing Guidelines for Cellular Mobile Services in Bangladesh*, (14.32.0000.702.41.062.19.42, 13 February 2024) <https://btrc.portal.gov.bd/sites/default/files/files/btrc.portal.gov.bd/page/1c1ea1c0_f8ef_4cdf_9005_d8a34b9ca554/2024-02-14-04-41-6270e029d094b61f9f411a16a8d3baab.pdf>.

21 Rumi Kawser, 'BTRC Blocks Webpage Containing Reports of Abuse BUET', *Dhaka Tribune*, (Dhaka, 10 October 2019) <https://www.dhakatribune.com/bangladesh/dhaka/189873/btrc-blocks-webpage-containing-reports-of-abuse-in>.

entitled to have a Corporate Policy Standard in line with international human rights principles. The problem arises when corporate policies that are in line with international human rights norms conflict with the domestic law of the country where the companies are operating. Complying with a government order just because it is the law of the land, even though such compliance can result in a gravely negative impact on human rights, makes a corporate entity an "enabler" of the human rights violation being committed. In situations like these, corporations having more bargaining powers are expected to push back against unlawful government orders. In countries like Zimbabwe, Togo, India, Myanmar and Pakistan, there have been instances where telcos have already taken a legal stance against the government, or at least pushed back against such orders. Not all pushbacks have had positive outcomes.

Pakistan: In the case of *Benazir Bhutto v. Federation of Pakistan*[22], where the President's power to impose emergency rules was subject to judicial review, it was emphasized that, the judicial review of administrative actions can be exercised on the grounds of illegality, irrationality, procedural impropriety, and unreasonableness. Thus, as per this decision, an administrative order for Internet shutdowns may be the subject of judicial review. A landmark judgment in *CM Pak Limited Vs The* Pakistan Telecommunication Authority[23] outlines that the power to suspend or cause suspension of the services, operations or functions of a licensed telecommunication provider in the context of 'national security' is exclusively provided under section 54(3) of the Pakistan Telecommunication (Reorganization) Act 1996 (hereinafter "PTA"), and that it can only be invoked if there is a Proclamation of Emergency by the President of Pakistan pursuant to powers vested under Part X of the Constitution. The suspension of operations can, therefore, only be justified if the President exercises this power to proclaim an emergency. In this case, a policy directive issued under section 8 of the PTA of 1996 empowering the Authority to suspend the cellular services was held to be a blatant disregard to the provisions of section 54 and therefore unlawful. The same judgement provides that, causing the suspension otherwise, other than by emergency power of the President under Section 54(3) may expose the Federal Government or the Authority to claims of compensation or damages by the licensees or the users of the mobile cellular services.

This case portrays the legal protection Pakistani Telcos enjoy against arbitrary administrative orders for Internet shutdowns. Essentially, they can rely on this decision to refuse to comply with an order of Internet shutdown in all situations except when an emergency is proclaimed by the President of Pakistan.

Zimbabwe: In a landmark move in 2019, in the *case of Zimbabwe Lawyers for Human Rights v Minister of State in* the President's office for National Security,[24] *government* authorities who had issued arbitrary Internet shutdown orders were officially accused of bullying Internet services providers into complying with their unreasonable and politically motivated directives, such acts eventually being declared unlawful. However, given control of the government over the International Gateway system and every intent of the government to wield the sword over

22 *Mohtarma BENAZIR BHUTTO and another v PRESIDENT OF PAKISTAN and others* (1988) PLD 1988 SC 416.

23 *CM Pak Limited v The Pakistan Telecommunication Authority* (2017) HCJD/C-121.

24 *Zimbabwe Lawyers for Human Rights and Media Institute of Southern Africa v The Ministry of State in the President's Office Responsible for National Security, Director General of Intelligence, Presid*ent of The Republic of Zimbabwe, Econet Wireless (PVT) Limited and Telecel Zimbabwe (PVT) Limited (2019) HC 265/19.

telcos through restricting speed, accessibility, and availability of Internet traffic, the government retains control and conducts digital authoritarianism.

Togo: In a case of *Amnesty International Togo & 7 Ors v Togo*[25], it was opined that, despite national security being a valid defence to derogate from certain rights, it must be done in accordance with the law. In this case, the respondent's argument was that the Internet shutdown was necessary to resist a protest that had the potential to turn into a civil war. While the argument was considered to have merit, the court held that since the action was done without valid legislation, it was therefore illegal, despite the necessity of the situation. This case highlights how human right requirements were prioritized over national interest.

Myanmar: The situation in Myanmar is a classic story of pushback against the government, where the telco ultimately had to exit, leading to backlash from critics, who called it a "cut and run". The government in Myanmar demanded real-time surveillance on its citizens, metadata, call-recording capabilities and back-door access to encrypted traffic. These demands were in contravention of Norwegian laws and EU privacy laws, including the General Data Protection Regulation (GDPR). Before the coup of February 2021, telecom and internet service providers had been secretly ordered, months before the coup, to install intercept technology that would allow the army to eavesdrop on the communications of citizens.[26] Ultimately, On July 8, 2021, Telenor made announcements of selling its Myanmar units to Lebanon's M1 Group for USD 105 million.[27] That deal formally closed in March 2022. With the exit of Telenor, only one (1) non-state backed telco remained in Myanmar.[28] Many criticized the move and called out for a "responsible exit", following the best practices under United Nations Guiding Principles on Business and Human Rights (UNGPs) and OECD Guidelines for Multinational Enterprises (OECD Guidelines) requiring rigorous, context-specific due diligence, communication and consultations with all relevant stakeholders in meaningful and timely manner and seeking advice from all credible, independent experts[29].

The lessons therefore are that despite some instances of legal action taken against unlawful, arbitrary and unreasonable Internet shutdown orders, telcos are still bound by domestic laws of the countries they operate in, and subject to the states' mandates for internet regulations. When a state has a legal framework that enables Internet shutdowns and calls for a shutdown under that specific framework, telcos are bound to follow that order as it is mandated by a valid law or regulation. Despite the existence of some safeguards against arbitrary internet shutdown orders, the reality is that regulations are often interpreted and implemented in a

25 *Amnesty International Togo, L'Institut Des Medias Pour La Democratie Et Les Droit De L'Homme, La Lanterne, Action Des Crechretiens Pour L'Abolition De La Torture, Association Des Victims De Tortur Au Togo, Ligue Des Consommateurs De Togo, L'Association Togolaise Pour L'Education Aux Droits De L'Homme Et La Democratie and Houefa Akpeda Kouass v The Togolese Republic* (2020) ECW/CCJ/JUD/09/20.

26 Rina Chandran, 'FEATURE-A year after Myanmar coup, growing surveillance threatens lives'. *Reuters* (31 January 2022) <https://www.reuters.com/article/business/media-telecom/feature-a-year-after-myanmar-coup-growing-surveillance-threatens-lives-idUSL8N2TX2KI/>.

27 ibid 19.

28 'Telenor's exit from Myanmar leaves behind safety and human rights questions' *Access Now*, (Web Page, 26 January 2023) <https://www.accessnow.org/press-release/telenor-exits-myanmar/>.

29 Joseph Wilde-Ramsing, Katharine Booth, Audrey Gaughran, 'Telenor's exit from Myanmar – a cautionary tale for the just transition' *SOMO* (Web Page, 27 September 2021) <https://www.somo.nl/telenors-exit-from-myanmar-a-cautionary-tale-for-the-just-transition/>.

manner so as to weaponize shutdowns. Many shutdown orders take place because authoritarian regimes want to suppress dissent and curtail civil rights of its citizens.[30] While these shutdown orders negatively impacted the telecommunication companies, many a time, instead of resisting orders, these companies become "enablers", as seen in the case of Myanmar, where the company Telenor exited the country on grounds of human rights, but was called out for an irresponsible exit as it sold its telecom units to Lebanon-based M1 and Myanmar's Shwe Byain Phyu Group, an entity with close ties to the Myanmar military.[31]

4. DISCUSSION AND IMPLICATIONS OF CASE STUDY

Telcos have long voiced a particular concern: how is a company to be blamed for adhering to government orders mandated by the law of the land? If anything, the government is to be blamed for the shutdown order and subsequent human rights violations. How is the corporation responsible? Also, under what law can corporations be held liable?

The companies often argue that the Internet shutdowns are carried out by ISPs under the orders of the government, which has unfettered control over them. Since the whole internet gateway system is controlled by the government, Telcos have little to do in these situations. Freyburg and Garbe (2017) highlight that original data on ISP ownership structures and documented Internet shutdowns reveal a positive relationship between companies that are primarily owned by an authoritarian state and the halt of Internet provisions within that state.[32] They argue that Internet shutdowns may be facilitated even if privately owned ISP investors have close ties to the ruling elites, despite being foreign investors.[33]

Companies also have a long-standing contention that their entire business model is heavily dependent on operating licenses, and government threats to rescind or withdraw this license for not adhering to regulatory protocols, and the companies' intention to sustain their license at all costs, have been major incentives to abide by any shutdown orders.

Many of these companies also argue that government ownership in Telecom Companies enable the State ordered shutdowns and such Companies themselves are bound by management decisions into following the Government Orders. However, these situations beget the question of the responsibility of private Telcos in ongoing unreasonable government shutdown orders, though they are also susceptible to the threat on operating licenses and often argue that they are arm-twisted into following the orders.

The exit of Telenor in Myanmar back in 2023 called out on their irresponsible exit for not leaving another alternative responsible telecom group to take the place of Telenor. However, Telenor argues that it had really had only three choices at that time – to adhere to

30 Rich Haridy, 'How governments shut the internet down to suppress dissent', New Atlas, (Melbourne, 26 February 2020) https://newatlas.com/telecommunications/internet-shutdown-global-report-access-now/.

31 Tina Freyburg, Lisa Garbe, 'Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa' (2017) 1932–8036/20180005 *International Journal of Communication* 12 <https://www.bing.com/ck/a?!&&p=86d7a0fcba97f18a870db2cd4669e83a10945376eb22b6d63c8ab712769a0901JmltdHM9MTc1NDAwNjQwMA&ptn=3&ver=2&hsh=4&fclid=230609dc-fd59-6d04-2aa9-1d46fcc26cdc&psq=Blocking+the+bottleneck%3a+Internet+shutdowns+and+ownership+at+election+times+in+sub-Saharan+Africa.+International+Journal+of+Communication%2c+12%2c+3896%e2%80%933916.&u=a1aHR0cHM6Ly9pam9jLm9yZy9pbmRleC5waHAvaWpvYy9hcnRpY2xlL2Rvd25sb2FkLzg1NDYvMjQ2NA&ntb=1>.

32 ibid 23.

33 ibid 23.

government orders and hand over private user data; or to resist the government orders and risk prison time, arrest and torture of its employees; or to sell its shares to a company not bound by EU Data Protection policies and regulations at the cost of making its User Data vulnerable and susceptible to military surveillance. Telenor chose option 3 as the best option to save its employees from a dire fate and to also to save itself from the liability of handing over sensitive data to the junta. However, Telenor's act of knowingly selling its units to a Company that did not have an internal policy requirement to uphold the same standard of 'User Confidentiality', earned itself a complaint from 474 Myanmar based civil society organizations to the Norwegian contact point for the OECD under the OECD Guidelines for Multinational Enterprises.[34]

4.1 Bangladesh and the Internet Shutdown in July 2024

Between 17-28th July 2024, Bangladesh faced a nationwide Internet shutdown, and consequently, digital repression. According to the 2024 Country Reports on Human Rights Practices: Bangladesh, published by the US Department of Justice, police and intelligence agencies under the previous government continued to threaten, and harass, and subject human rights defenders, civil society leaders, and the family members of critics based outside of the country under surveillance throughout July. Journalists living abroad reported police and intelligence agencies had harassed and intimidated their relatives in the country to silence criticism.[35] The following discussion is on the possible legal arenas these telcos could navigate in order to mitigate future internet shutdown orders so that July 2024 and the internet blackout period does not repeat itself in Bangladesh.

4.2 Corporate Criminal Responsibility

According to Ambach (2011), corporates may incur liability to international crimes if the services they provide or refrain from providing where they are to provide services - are used to commit international crimes such as war crimes, crimes against humanity or genocide.[36] International criminal liability of corporations for business transactions regarding complicity in atrocities and facilitating grave crimes has previously been observed in the cases of *United States v. Friedrich Flick* and *United States v. Carl Krauch.*[37] In the *United States v. Friedrich Flick case*, the corporate veil was lifted to hold industrialist Friedrich Flick and his executives personally liable for war crimes, such as the systematic use of slave labor, that were executed through their corporation. In *United States v. Carl Krauch*, the directors of the IG Farben conglomerate were held personally accountable for crimes against humanity, including the production of Zyklon B gas for extermination camps, carried out under their corporate authority. These cases illustrate, Corporations, or rather the people behind

34 OECD National Contact Point, 'Memorandum of Understanding between Telenor and SOMO' (Web Page, undated) <https://files.nettsteder.regjeringen.no/wpuploads01/sites/263/2022/10/OECDNCP_Telenor_SOMO_MoU_12J>

35 US Department of State, '2024 Country Reports on Human Rights Practices: Bangladesh' (Web Page, 2024) <https://www.state.gov/reports/2024-country-reports-on-human-rights-practices/bangladesh>

36 Philipp Ambach, 'International Criminal Responsibility of Transnational Corporate Actors Doing Business in Zones of Armed Conflict' in Freya Baetens (ed), Investment Law within International Law: Integrationist Perspectives (Cambridge University Press, 2013) 51–82; *Rome Statute of the International Criminal Court* (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 90, arts 6–8.

37 Trial of Friedrich Flick and Five Others (1947) 48 United States Military Tribunal, https://www.worldcourts.com/imt/eng/decisions/1947.12.22_United_States_v_Flick2.pdf; Trial of Carl Krauch and Twenty-Two Others (1947) 57 United States Military Tribunal https://www.worldcourts.com/imt/eng/decisions/1948.07.29_United_States_v_Krauch.pdf.

them can be made liable for knowingly enabling gross Human Rights violations, or facilitating international crimes.

The role of telcos though may not be as actual perpetrators of commission of crimes, but they can be accessories (i.e., those who assist the principals in the commission of a crime) to such crime as established in *Lubanga case*.[38] According to *Lubanga* the distinction between a co-perpetrator and accessory is that of control and all participants share control over the crime because each of them could frustrate its commission by not carrying out his or her task.[39] This provides a possible avenue for accountability and individual criminal responsibility of the people behind the telcos, though a more robust analyses will likely reveal substantial hurdles in doing so.

During the July 2024 Internet Shutdown order in Bangladesh, the telcos in Bangladesh were mostly silent on the topic of Internet Shutdown order even though it directly affected their business incurring a loss of billions of dollars. The major actors of Telcos in Bangladesh are Grameenphone (a subsidiary of Norway based Telenor); Robi (jointly owned by Axiata Group of Malaysia, Bharti Airtel of India); and Banglalink Digital Communications Ltd. (fully owned by VEON Ltd. Netherlands); Teletalk Bangladesh Ltd. (Government owned telco in Bangladesh). The only form of protest came from Grameenphone Bangladesh's parent company, Telenor Asia, where on 4th of August 2024, it issued a public statement expressing "deep concern" over the shutdown and urged the Bangladesh government to immediately and fully restore mobile internet services.[40] They also issued regular updates on broadband services provided during the lockdown period.[41] Interestingly, all these Telcos (except Teletalk) despite being mostly foreign owned chose to stay silent and chose business over taking a stance. Since these companies were the major players in the telco sector, if all these companies were pushed back by refusing to comply with unlawful orders, the government couldn't have cancelled licenses of all the Telcos altogether since doing so would have collapsed the communication system of the country. Thus, by willingly abiding by government orders knowing fully well that there are instances of state-backed atrocities being committed on protestors during internet blackout period and there is virtual certainty that such atrocities can be committed,[42] telcos heads may possess *dolus eventualis*. Whether or not this mode of liability apply to Bangladeshi telcos is subject to further research. However, given that the companies are continuing their business since July 2024 primarily suggests that they bear no individual criminal responsibility.

4.3 Case in International Courts

Because corporations including Telcos are not subjects of international law, they cannot directly go to International Courts such as the International Court of Justice, or the European Court of Human Rights. The International Criminal Court only allows individuals as a party and WTO Dispute Settlement Board only

38 The Prosecutor v Thomas Lubanga Dyilo (2007) ICC-01/04-01/06, 410.

39 ibid, 31

40 TBS Report, 'Telenor Asia Urges Full Restoration of Mobile Internet in Bangladesh' (The Business Standard, 4 August 2024) <https://www.tbsnews.net/bangladesh/telecom/telenor-calls-immediate-full-restoration-mobile-internet-services-909836>

41 Telenor Asia, 'Situation in Bangladesh' (Web Page, 5 August 2024) <https://www.telenorasia.com/announcements/situation-in-bangladesh/>

42 *Prosecutor v. Thomas Lubanga Dyilo* (Judgment on the appeal of Mr Thomas Lubanga Dyilo against his conviction) ICC-01/04-01/06 A 5 (1 December 2014) para 6.

allows member states as litigants. However, the nation-state where the parent company is incorporated, can go to ICJ asking for unlawful threats and pressure on its 'legal citizens' i.e., the Telco. For example, Telenor, which is the parent company of Grameenphone in Bangladesh, is registered in Norway. As the nation-state to the parent company, Norway may go to International Courts on behalf of its company against the nations where Telenor faces backlash from the Authoritarian regime for taking a stance against unlawful orders or at least take an Advisory Opinion against the Authoritarian regimes from the ICJ.

4.4 Erga Omnes: Obligation of other states against Authoritarian government

Erga Omnes is the obligations owed to all of the international community as a whole towards some violations that have worldwide outreach or 'legal interest'. It was established in the *Barcelona Traction* decision of 1970 that, the obligation of States towards the international community as a whole,[43] distinguishing it from obligations arising towards individual states. The obligations falling under customary international law falls within the scope of 'legal interest' of '*Erga Omnes*' as enumerated in the proceedings by Marshall Island against India[44], Pakistan[45] and the United Kingdom[46]. In this case, Marshall Island, in April 2014, instituted suits before the ICJ on the failure of the countries to fulfil its customary international law obligation enshrined under the treaty of Non-Proliferation of Nuclear Weapons (NPT), 1978. Despite India and Pakistan not being a party to the treaty, ICJ accepted the jurisdiction under Customary International Law violation. Now, using Internet Shutdown as a weapon to commit mass atrocities falls under the violation of the highest form of Customary International Law, i.e. *Jus Cogens*. Therefore, any state not necessarily having Business in a specific Authoritarian regime should consider taking a case in ICJ either as a contentious case or as an Advisory Opinion at the very least, if Telco nation-state countries refuse to go forward with a formal proceeding. We know of the state-backed atrocities committed during July 2024 by the government in Bangladesh. The justiciability and the legality of the Internet Shutdown during July and the atrocities committed during internet blackout period, could be an issue that could be taken to International Court by any nation that is a nation-state to a telco parent company regardless that telco having business in Bangladesh or not.

5. CONCLUSION

Being a direct actor involved in internet shutdowns, and in light of corporate human rights responsibilities, telcos have an active duty to ensure that their activities, including complying with government orders do not violate, or facilitate the violation of human rights. While rights of freedom of expression and privacy are not absolute, any limitation to them must be legal, necessary and proportional. Unless the orders fulfil all three of these elements, telcos must resist the orders within their abilities. However, the accountability mechanism, when telcos fail to fulfil this responsibility and end up facilitating gross human rights violation stands on shaky grounds. Corporate criminal responsibility is

43 Case Concerning the Barcelona Traction, Light and Power Company, Limited Belgium v Spain (1970) ICJ Rep 32.

44 Obligations concerning Negotiations relating to Cessation of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Islands v India) (Application) [2014].

45 Obligations concerning Negotiations relating to Cessation of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Islands v Pakistan) (Application) [2014] par 2.

46 Obligations concerning Negotiations relating to Cessation of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Islands v United Kingdom) (Application) [2014]

rarely invoked, because the telcos hold substantial leverage on developing states, preventing the possibility of prosecution. Individual criminal responsibility under Rome Statute too does not become relevant unless there is substantial evidence as to the telco heads' specific intent to facilitate the commission of international crimes, and the crime meets certain intensity and gravity threshold. In terms of the accountability of states for illegal orders of internet shutdowns, a case before the ICJ is an option, though very unlikely to be utilized, as it depends on state consent. Overall, the accountability mechanism regarding the whole scheme of illegal internet shutdowns is inadequate, and the telcos are left in a precarious position where they have to protect their business interest, comply with domestic laws, and also have to comply with their human rights obligation. When these responsibilities conflict, the telcos too are left without legal protection. A case study of the internet shutdown in Bangladesh during July-August of 2024 brings all these concerns to the fore. While the responsibility of telcos in Bangladesh in that period is unclear, the telcos are left unprotected for any similar situations in future, and the government too bears no responsibility for illegal internet shutdown orders.

WOULD COMMUNITY NOTES WORK IN BANGLADESH?

Tackling Political and Gender-Based Misinformation

Afrida Samiha Nabilah

Abstract

Meta's Facebook, one of the most popular social media platforms, is also a major source of information in Bangladesh. However, it is often exploited to spread misinformation or fake news, frequently targeting political opponents and women. While this issue is already a serious concern for policymakers and stakeholders, Meta's recent decision to replace professional fact-checkers with a user-driven system such as Community Notes in some parts of the world has raised additional, significant questions. This study seeks to explore the consequences of such a move by Meta and to examine whether Community Notes can effectively combat misinformation in the Bangladeshi context.

This study analyzed qualitative data from expert interviews to examine the impact of Community Notes. Findings show the system is vulnerable to abuse by political groups, lacks local language expertise, offers limited transparency, and may disadvantage women and minorities. Without professional oversight, misinformation could spread unchecked.

The study concludes that Community Notes, in its current form, is not adequately equipped for Bangladesh's complex digital landscape. It recommends a hybrid model that combines trained moderators with community input. It also calls for expanding language coverage, ensuring transparency, engaging local civil society and strengthening accountability mechanisms.

1. BACKGROUND

Social media platforms, such as Facebook, YouTube, etc., have become a powerful part of modern digital public life and Bangladesh is no exception. Social media is the first place that netizens turn to for news. However, this reliance also creates space for misinformation, especially during elections, communal tensions, and moments when public trust is most fragile.[1]

Meta's Facebook, the most widely-used social media platform in Bangladesh, plays a key role in how people access news media, express opinions, and share information.[2] In December 2016, Meta introduced third-party fact-checking as one of its content moderation systems, which continued until the company's decision to end it in January 2025,[3] with complete withdrawal eventually taking place by April of the same year. Changes in content moderation on this platform can shape public trust, and influence how information is received.

Facebook has more than 67 million users in Bangladesh as of February 2025.[4] Facebook's immense reach, globally, forced Meta to address content accuracy by implementing its system of third-party fact-checkers. As a part of this process, Meta also partnered with professional fact-checkers in Bangladesh. Organizations like Rumor Scanner Bangladesh were engaged with verifying content and exposing false claims.[5] For instance, Rumor Scanner Bangladesh detected 2,919 false claims in 2024, up from 1,915 in 2023. Of these, 2,330 cases were on Facebook alone, which means over six false posts were detected every day.[6]

But as of early January 2025, Meta decided to replace this third-party fact-checking system with Community Notes in the USA, on the grounds that fact-checkers were too politically biased and made too many mistakes, arguing the system had become a tool for censoring legitimate speech and had thus lost public trust.[7] The Community Notes is a user-driven tool inspired by Elon Musk-owned X (formerly Twitter).[8] The tool leaves it up to volunteer users to add contextual notes rather than having trained professionals debunking false claims. Under this system, users themselves can write notes under posts they believe are misleading. If enough people support the note, it then becomes visible.

Reports suggest that popular mass media were unable to perform their roles effectively during the tenure of the previous government, because they had become overly politicized. Therefore, Meta's shift from a third-party fact-checking system to Community Notes is significant, as Facebook plays a crucial role in

1 LIRNEasia, *Misinformation in Bangladesh: A Brief Primer* (Report, LIRNEasia, October 2021) 1

2 Niemur Rahman Emon, 'Facebook journalism fuels country's scroll media boom' *Daily Observer* (Web Page, 4 July 2025)

3 'Meta Ends Fact-Checking in the U.S.: Legal and Political Implications' (DDG)

4 NapoleonCat, *Facebook users in Bangladesh – February 2025* (Web Page, February 2025) <https://napoleoncat.com/stats/facebook-users-in-bangladesh/2025/02/>

5 Rumor Scanner Bangladesh (Web Page, March 2020) <https://rumorscanner.com/about-us>

6 Rumor Scanner Bangladesh, *Statistics of Rumors in 2024* (Web, 2024) <https://rumorscanner.com/en/statistics-2/rumors-data-2024/134624>

7 Al Jazeera, 'Meta, Facebook to drop fact-checkers: What does this mean for social media?' (January 2025) <https://www.aljazeera.com/news/2025/1/10/meta-facebook-to-drop-fact-checkers-what-does-this-mean-for-social-media>

8 ABC News, 'Elon Musk created Community Notes and Meta is following suit. Here's how it works' (8 January 2025) https://www.abc.net.au/news/2025-01-08/elon-musk-community-notes-on-meta-facebook-explained/104794984

the Bangladeshi media and information landscape, where many people rely on it for news and public debate. A recent survey found that 74% of in-person and 84% of online respondents rely on social media for news, with Facebook being the most used platform.[9] Any change in the platform's content moderation thus has a direct impact on how information is shared, consumed, and trusted.

Meta argues that this shift supports free expression and reduces political bias.[10] The company also claims that it encourages free speech and helps build trust by letting users participate directly in content moderation.[11] Under the new approach, only "high-severity" violations are enforced, which allows at least some of the misleading content to stay online.[12] Meta also justifies these steps as protecting free expression. Global research confirms that the new Community Notes system fails to stop misinformation because political opponents can easily coordinate to prevent fact-checking notes from appearing.[13] This system is slow as well as structurally vulnerable, which can contribute to the platform's inability to protect women and vulnerable groups against targeted abuse.[14]

However, experts argue that this outright shift risks accountability, suggesting that it could instead be incorporated as an additional component of the platform's information moderation system.[15] Rights organizations such as Access Now and Article 19 have warned that reducing professional oversight increases the risk of unchecked hate speech, disinformation, and attacks on marginalized communities.[16] Decentralized systems also lack expertise to tackle culturally specific misinformation. This shift, like many other aspects of social media, aligns with a broader global trend. Figures like Donald Trump claim that fact-checking limits speech.[17] A statement as such undoubtedly plays a role in shaping global political narratives on this issue. It also aligns with Meta's decision to limit content moderation and unchecked spreading of misinformation, which might be harmful as well.

But it is still unclear how this will work in Bangladesh. Although the number of internet users is on the rise, there is an absence of measures taken to verify things that people see online. Studies show that a large portion of users passively use social media without any

9 Dhaka Tribune (online, 12 September 2024) <https://www.dhakatribune.com/bangladesh/372105/survey-most-youths-prefer-social-media-for-news>

10 Nicholas Reimann et al, *Meta uses Elon Musk's X algorithm for its new community notes* (News, 13 March 2025) <https://www.businessinsider.com/meta-community-notes-elon-musk-x-algorithm-facebook-instagram-2025-3>

11 ABC News (n 8)

12 MSU Today, 'What Meta's New Fact-Checking Policies Mean for Misinformation and Hate Speech' <https://msutoday.msu.edu/news/2025/ask-the-expert-what-meta-new-fact-checking-policies-mean-for-misinformation-and-hate-speech>

13 Augenstein, I., et al. (2025). Timeliness, Consensus, and Composition of the Crowd: Community Notes on X

14 Chuai, J et al., 'Did the Roll-Out of Community Notes Reduce Engagement With Misinformation on X/Twitter?' (2023) ResearchGate

15 Chris Vallance, 'Meta Wants X-Style Community Notes to Replace Fact Checkers — Can It Work?', BBC News (online, 26 January 2025) <https://www.bbc.com/news/articles/c4g93nvrdz7o>

16 Access Now, 'Meta's Abandonment of Fact-Checking Threatens Global Election Integrity' https://www.accessnow.org/meta-fact-checking-removal-threatens-elections ; Human Rights Watch, 'Misinformation and Hate Speech Online: A Global Crisis' https://www.hrw.org/news/2023/12/07/misinformation-hate-speech-online-global-crisis

17 LSE Grantham Institute, 'The Myth of Meta's Free Speech Places Democracy at Risk' <https://www.lse.ac.uk/granthaminstitute/news/the-myth-of-metas-free-speech-places-democracy-at-risk/>

critical engagement.[18] This makes the spread of false content easier, especially those designed to provoke outrage or reinforce existing political bias. This dynamic makes Bangladesh a unique case where misinformation here has repeatedly carried political and social consequences.[19] The country's fast digital growth has left most people without the skills to judge what they see online. This gap makes people vulnerable to being manipulated by made-up stories and inflammatory "*gujob*" (the local word for rumors).[20] For instance, a photoshopped image, that too uploaded from a hacked profile on Facebook, sparked mob violence in Ramu against the Buddhist community in 2012.[21] In 2019, false rumors about child abductions spread online and triggered mob attacks in several areas.[22] In recent years, political opponents and women have become key targets. False quotes, edited photos, and deepfakes are used to discredit opposition figures or shame women, particularly journalists and rights activists.[23] Such attacks exploit gender stereotypes and social stigma, silencing differing opinions and discouraging women's participation in public life.

In this context, the decision to introduce community-based moderation remains questionable, especially in the context of Bangladesh. It is yet to see whether the Community Notes feature can effectively function in Bangladesh. It also leaves questions about gaining people's trust, efficiently tackling misinformation and most importantly, who will be held accountable if the system fails. Since the tool is decentralized in nature, it is highly unlikely to be equipped with tackling religious, political and gender-based misinformation.[24]

Bangladeshi people have already seen examples of this during the July 2024 Uprising, when there were attempts to spread politically motivated disinformation campaigns from outside the country. False narratives were spread about a "Hindu genocide" to destabilize the interim government.[25] A tool run by regular users, without expert fact-checkers, would likely be ineffective against such complex and harmful campaigns.

This report attempts to explore the impact of this change introduced by Facebook in Bangladesh. It starts with the Background, which introduces the main topic of Meta's content moderation in Bangladesh. The Literature Review explains what misinformation looks like in the country and compares Meta's old and new moderation systems. The Methodology section describes how the research was conducted using qualitative data. The core sections of the report, the Findings and Discussion, highlight experts'

18 Yasin Shafi, *Digital Literacy and Access to Public Services in Rural Households of Bangladesh* (BIGD Report, August 2023) 12, 22–23<https://bigd.bracu.ac.bd/publications/digital-literacy-and-access-to-public-services-in-rural-households-of-bangladesh/>

19 A. Binte Towhid, *Misinformation in Bangladesh: A Brief Primer* (LIRNEasia, 2021)

20 ibid.

21 The Daily Star, 'Violence in Ramu: 10 yrs on, justice still pending' <https://www.thedailystar.net/news/bangladesh/crime-justice/news/violence-ramu-10-yrs-justice-still-pending-3130746>

22 The Daily Star, 'Bangladesh lynchings: Eight killed by mobs over false child abduction rumours' <https://www.bbc.com/news/world-asia-49102074>

23 Kundu, Priyanka and Mahbubul Haque Bhuiyan, 'Online Harassment of Female Journalists in Bangladesh: Forms, Reactions, and Consequences' in *Handbook of Research on Discrimination, Gender Disparity, and Safety Risks in Journalism* (IGI Global, 2021)

24 Antara Chakraborthy, 'How Cross-Border Disinformation Fuels Hate in Bangladesh and India' (2024) Center for the Study of Organized Hate

25 ibid.

concerns about the new Community Notes tool. Finally, the Recommendations and Conclusion provide specific suggestions for a better way forward and wrap up the core points.

2. LITERATURE REVIEW

2.1. Information and Right to Information

The concepts of information and right to information are fundamental to a healthy society. In Bangladesh, this right was officially recognized by the Right to Information Act, 2009, which was enacted to give citizens a legal way to access official information, a vital tool for accountability.[26]

However, a legal right to information does not stop misinformation being spread. The issue also often has a cross-border aspect where these are transmitted from outside the country. Following recent political unrest, disinformation campaigns from outside the country used false claims to inflame tensions and destabilize the government.[27] These are not simple rumors; they are complex campaigns that a user-based moderation system, without professional fact-checkers, would likely fail to counter.

Yet, access to information does not ensure access to accurate information. The digital space has made falsehoods travel faster than verified information.

2.2. Understanding Misinformation and Disinformation in Bangladesh

Misinformation refers to false information shared without intent to deceive or cause harm. On the other hand, disinformation is the spreading of false and fabricated news or information deliberately. In Bangladesh, both types are common on social media platforms like Facebook, YouTube and TikTok. Such posts often involve misleading headlines, photos and fake statements about public figures.

During the 2018 and 2024 general elections, false stories targeted opposition leaders and activists.[28] This caused confusion among voters and weakened trust in the election process. In Bangladesh, two types of misinformation and/or disinformation are most common, political disinformation and attacks against women online. Political posts often include fake quotes, edited photos, or false claims about elections and opposition leaders.[29] Women, especially journalists and rights workers, are frequently targeted with doctored content and moral attacks.[30] These trends increase during elections or public protests and can easily go unnoticed in a community-based system, especially when users aren't trained or don't understand the local context.

Internet use is rising fast in Bangladesh. While many people now rely on social media for news,[31] digital literacy remains low. Many

26 MRDI, *Right to Information Act: Structure and Application English* (2012) [2]; Transparency International Bangladesh (TIB), 'The RTI Act of 2009 Empowers Citizens to Combat Corruption' (2024) [3]

27 Niharika Sharma and Md Abdul Hasib Khan, 'Rumors, Fake News, Disinformation, Propaganda and Social Media Algorithm During (July–August 2024) Young Jihadists-Hostility: Content Producing and Diffusing Perspectives of Bangladesh' (Preprints.org, 2025)

28 Ibrahim bin Harun and Muhammad Anwarus Salam, 'Facebook as Political Campaign Tool: A Study on Election 2018 in Bangladesh' (2018) 8(1) *Journal of Social Science* 71.

29 Tohidul Islam Raso and Partho Protim Das, "Misinformation trends and narratives in Bangladesh's tumultuous 2024" Dismislab (Web Page, 21 January 2025).

30 Tech Global Institute, "From Homophobia to Assault: The Gendered Landscape of Bangladesh's Political Disinformation" (InfoLab Web Page, December 2023–January 2024) <https://infolab.techglobalinstitute.com/from-homophobia-to-assault-the-gendered-landscape-bangladeshs-political-disinformation/>.

31 Mehnaz Rabbani, Maria Matin, Iffat Zahan, Md Saiful Islam and Semab Rahman, Digital Literacy and Access to Public Services in Bangladesh (BRAC Institute of Governance and Development Web Page, 2019–2020) <https://bigd.bracu.ac.bd/study/digital-literacy-and-access-to-public-services-in-bangladesh/>.

users find it hard to distinguish real news from false content.[32] This makes Bangladesh especially vulnerable to the harmful effects of online misinformation.

For example, a persistent disinformation campaign has long circulated the "Padma Bridge rumor" in 2019. This falsely claimed that human heads were needed for the bridge's construction. This malicious rumor, which went viral on social media, triggered mob violence and resulted in the deaths of several people.[33]

Gender-based attacks are also widespread, often taking the form of technology-facilitated gender-based violence (TFGBV). These campaigns involve spreading deepfakes to harm women, using fake accounts to impersonate them, and doxing, which means exposing private information publicly.[34] Men are also targeted, often with gendered and homophobic insults that question their masculinity or political credibility by comparing them to transgender or homosexual individuals.[35] Such patterns align with broader regional research indicating that gendered and political disinformation frequently overlap, especially in polarized environments.

2.3. Impact of Misinformation and Disinformation During Crises

Misinformation is not only limited to political events. It also spreads widely during emergencies, like natural calamities, communal issues or public health crises. During the COVID-19 pandemic, misinformation spread widely across social media. False claims about vaccines causing infertility, and vaccination drives or the pandemic itself being a government conspiracy, circulated.[36] These rumors led to confusion, especially in rural areas and delayed government initiatives for vaccination. Similarly, during the 2022 Sylhet floods, social media platforms were inundated with misleading posts, including false warnings of more incoming disasters, and a few other allegations of biases on the part of authorities while distributing relief goods.[37]

In such situations, people rely on viral posts or videos which are rarely checked. This leaves the crisis communication system fragile and highly vulnerable for manipulation. These examples reveal that misinformation exploits public distrust.

2.4. The Role of Algorithms and Engagement Bias

Platforms are designed in a way that allows the drive of misinformation. Quite often, algorithms prioritize content that is filled with outrageous responses rather than true facts. Many existing studies show that misleading posts tend to have better reach on such platforms due to the outrage they create

32 ibid.

33 A. Binte Towhid (n 20).

34 Voices for Interactive Choice and Empowerment, 'Digitally Exposed: Technology-Facilitated Gender-Based Violence in Bangladesh – Trends, Cases, and Recommendations' (4 August 2025) <https://voicebd.org/2025/08/04/digitally-exposed-technology-facilitated-gender-based-violence-in-bangladesh-trends-cases-and-recommendations/>.

35 Tech Global Institute, 'From homophobia to assault: The gendered landscape of Bangladesh's political disinformation' (14 August 2024) <https://infolab.techglobalinstitute.com/from-homophobia-to-assault-the-gendered-landscape-of-bangladesh s-political-disinformation/>.

36 Ingjerd Skafle, Anders Nordahl-Hansen, Daniel S Quintana, Rolf Wynn and Elia Gabarron, 'Misinformation About COVID-19 Vaccines on Social Media: Rapid Review' (2022) 24(8) *Journal of Medical Internet Research* e37367, doi:10.2196/37367.

37 Dhaka Tribune, 'Fact Check: Flood-related Fake Photos, Videos Overwhelming Social Media' (*Dhaka Tribune*, 25 August 2024) <https://www.dhakatribune.com/bangladesh/355984/flood-related-fake-photos-videos-overwhelming-in>.

amongst a large number of people.[38] It is their business model that rewards misinformation.

But the spread of such misinformation is becoming dangerous day by day, especially in the South Asian region, where internet use is rising but digital literacy remains limited. Algorithms make this worse. Before the 2024 national elections in Bangladesh, Facebook and YouTube were flooded with deepfakes and fake news. These platforms amplify content that gets strong reactions, creating echo chambers and deepening political divisions. Emotionally charged and polarizing content, including violent speech, the fastest, sometimes leading to real-world mob violence.[39] The same happens with gendered attacks through photoshopped photos and deepfakes targeting women journalists and activists, goes viral because algorithms reward content that sparks outrage.[40] This system fuels the escalation of online attacks on women.

2.5. Content Moderation Before Community Notes

Before 2016, Meta's (then Facebook) way of dealing with false or harmful content was pretty basic. It relied on its own moderation teams, automated systems, and users reporting posts. There were no outside fact-checkers, or any independent verification. But after December 2016, the platform announced that it would start working with third-party fact-checkers like ABC News, the Associated Press, FactCheck.org, PolitiFact, and Snopes.[41] Over time this expanded into a global program, with partners certified by the International Fact-Checking Network (IFCN).

In Bangladesh, Meta partnered with third-party fact-checkers like AFP Fact Check and BOOM Bangladesh, which were part of the IFCN.[42] Organizations like AFP Fact Check and BOOM Bangladesh verified online content and labeled those based on accuracy.[43] Meta would reduce its reach and attach warning labels when a content was marked as false or misleading.[44]

Along with fact-checking, Meta employed automated detection tools and moderations teams to remove content that went against their community standards.[45] However, these methods were not flawless. Fact-checkers also had limitations. Some false content slipped through due to lack of resources or political pressure on them, based on geographic location.[46]

38 Sundar Sarukkai, 'Algorithms and Misinformation: A Philosophical Analysis', *Economic and Political Weekly* (Vol 56, Issue 20, 2021) 24.

39 Niharika Sharma and Md Abdul Hasib Khan (n 27).

40 Voices for Interactive Choice and Empowerment, 'Digitally Exposed: Technology-Facilitated Gender-Based Violence in Bangladesh – Trends, Cases, and Recommendations' (4 August 2025) <https://voicebd.org/2025/08/04/digitally-exposed-technology-facilitated-gender-based-violence-in-bangladesh-trends-cases-and-recommendations/>.

41 Sam Thielman, 'Facebook to Fact-Check, Label and Demote Fake News' *The Guardian* (15 December 2016) <https://www.theguardian.com/technology/2016/dec/15/facebook-flag-fake-news-fact-check>.

42 Financial Express, 'Facebook adds AFP, Fact Check to fact-checking programme in Bangladesh' (The Financial Express, 24 May 2021) https://thefinancialexpress.com.bd/national/facebook-adds-afp-fact-watch-to-fact-checking-programme-in-bangladesh-1621923851.

43 Barek Hossain, V L Muzykant and Md Nahiduzzaman, 'Roles of Fact-Checking Organizations in Bangladesh to Tackle Fake News' (2022) 5 *Law and Authority* 3.

44 Tessa Lyons, 'Hard Questions: What's Facebook's Strategy for Stopping False News?' (28 June 2018) *Meta Newsroom* <https://about.fb.com/news/2018/06/hard-questions-fact-checking/>.

45 Evelyn Douek, 'The Rise of Content Cartels', (2022) 121 *Columbia Law Review* 715.

46 Global Witness, 'Facebook's Content Moderation in the Global South' (Report, 2022) <https://www.globalwitness.org/en/campaigns/digital-threats/facebook-moderation-south/>.

2.6. Meta's Shift to Community Notes: Key Changes

In January 2025, Meta announced a major change in their content moderation. It removed many professional fact-checkers globally. The company claimed of allowing more speech and lesser mistakes caused by the previous content moderation system.[47] It introduced Community Notes, a crowdsourced moderation tool. This new system borrows from X: users can volunteer context under posts they find misleading.[48] A note only appears if contributors with differing viewpoints agree it's helpful, Meta itself doesn't write or decide which notes go live.[49] But Mark Zuckerberg argued that the old fact-checking model sometimes blocked legitimate speech and made errors. Community Notes, he said, would fix this by letting more people take part and by flagging only the most serious cases of harmful content.[50]

Community notes let users add notes to posts they believe to be misleading. These notes show only when users with diverse views agree on their accuracy.[51] Meta claimed this was more transparent and freer from political bias. It also argued that the new system promotes free speech and combats misinformation.

But experts raised concerns. Research shows that community moderation may be slow, inconsistent and lack visibility.[52] The risks are especially high in countries like Bangladesh due to existing political polarization and lack of digital literacy.[53] A report from BBC noted that Community Notes often fail to respond during crises and meanwhile the damage has already been done,[54] as Community Notes depend on volunteers who may not have specialized training or local knowledge.[55] This system's reliability is still unproven in complex contexts like Bangladesh.

Media reports have previously highlighted issues with Twitter's (now X) Community Notes. Delays in flagging harmful posts and uneven showing up of such notes are the most common.[56] However, Meta's shift may reduce expert input in identifying such content. This raises questions about how effective this new system will be, especially where political tension and limited digital literacy persists.

2.7. Problems with Community Notes in the Context of Bangladesh

The effectiveness of Community Notes in Bangladesh is limited by several factors. Firstly, the assumption that the user base out here is highly active but untrained.[57] Misleading claims, especially the political and religious ones can be difficult for an average

47 Joel Kaplan, 'More Speech and Fewer Mistakes' (Meta Newsroom, 7 January 2025) <https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/>

48 ibid

49 Testing Begins for Community Notes on Facebook, Instagram and Threads (Meta Newsroom, 13 March 2025) <https://about.fb.com/news/2025/03/testing-begins-community-notes-facebook-instagram-threads/>

50 ibid

51 ABC News (n 8)

52 ABC News (n 8)

53 BBC News, 'Why Meta Is Being Criticised for Dropping Fact-Checkers', *BBC* (online, 12 January 2025) <https://www.bbc.com/news/articles/cly74mpy8klo>

54 ibid

55 ABC News (n 8)

56 BBC News, Facebook and Instagram get rid of fact checkers (BBC News, 8 January 2025) <https://www.bbc.com/news/articles/cly74mpy8klo>

57 TBS Report, 'Digital Literacy Holds the Key to Digital Bangladesh: Banglalink Chief' (The Business Standard, 21 July 2019) <https://www.tbsnews.net/bangladesh/telecom/digital-literacy-holds-key-digital-bangladesh-banglalink-chief>

user to detect or verify.[58] Many users often lack basic skills to check sources, verify images, or recognize coordinated misinformation.[59]

Secondly, politically or religiously motivated groups can abuse the system. Groups may coordinate to promote or suppress certain narratives through mass sharing and voting on notes.[60] This allows misinformation to be validated by consensus. Because, online spaces are often seen dominated by groups who can shape the narratives they wish to establish.[61] As a result, a user-driven moderation system may repeat the same biases it aims to correct. In other words, the new content moderation tool may legitimize harmful content rather than debunking it.

Thirdly, language diversity is a barrier. Content in dialects from places such as Sylhet, Chittagong, Rangpur etc. may go unchecked due to lack of expertise in such dialects.[62] posts in these dialects or in Bangla-English mixed terms often confuse moderators from other regions. This lets false or harmful content spread within the regional communities. Thus, misinformation targeting regional communities remains unaddressed.

Fourthly, the selection criteria for note contributors is not transparent. It is unclear how users are selected to add notes, or removed from the process. It is also unclear what safeguard exists to prevent manipulation.[63] The lack of accountability and transparency weakens trust in the system.

Lastly, the system allows platforms like Meta to avoid responsibility by claiming that the content decisions are community-led.[64] This removes pressure on professional moderation and puts the burden back on users. In a context like Bangladesh where digital literacy is low, language is diverse, user-based moderation alone cannot ensure fairness or accuracy.

2.8. Concerns from Digital Rights Groups

Digital rights experts have played an important role in advocating for stronger platform accountability. Reports from organizations such as Access Now and Article 19 have warned that reducing professional oversight could increase the risk for vulnerable communities.[65] Experts argue that platform design, algorithm bias and weak regulation mechanisms contribute to the unchecked spread of misinformation. Their perspectives are essential to understanding the broader issues in social media governance in politically sensitive environments.

Rights groups have particularly warned that weak or relaxed content moderation policies could undermine security of minority

58 Md Mahfuzul Haque et al, 'Combating Misinformation in Bangladesh: Roles and Responsibilities as Perceived by Journalists, Fact-Checkers, and Users' (2020) 4(CSCW2) *Proceedings of the ACM on Human-Computer Interaction* 130, doi:10.1145/3415201

59 Mobassera Fatima, Barek Hossain and Valerii Muzykant, 'An Overview of Digital Media Literacy in Digital Bangladesh' (2023) 11(2) Jurnal Cita Hukum 267.

60 UNHRC, 'Human Rights and Social Media Platforms', (2023)

61 Valerii L Muzykant, Barek Hossain, Munadhil Abdul Muqsith and Mobassera Jahan Fatima, 'Media Literacy and Fake News: Bangladesh Perspective' (2022) 10 Jurnal Cita Hukum 223

62 Center for the Study of Organized Hate (CSOH), 'X's Community Notes and the South Asian Misinformation Crisis' (Report, 30 June 2025) <https://www.csohate.org/2025/06/30/x-community-notes-south-asia/>

63 Centre for Governance Studies, 'Digital Policy and Electoral Integrity', (2024)

64 European Democracy Hub, 'Big Tech Is Avoiding Responsibility' (European Democracy Hub, 30 June 2025) <https://europeandemocracyhub.epd.eu/big-tech-is-avoiding-responsibility/#:~:text=Meanwhile%2C%20Meta%20changed%20its%20content,propaganda%20that%20benefits%20its%20owners>

65 ARTICLE 19, 'The Failure of Platforms to Protect Freedom of Expression Online' <https://www.article19.org/resources/platform-responsibility-freedom-of-expression/>

communities leaving them exposed to online harassment.[66] Amnesty International reports that when platforms ignore hate speech, women, minorities and activists are often the first to suffer.[67] The United Nations Human Rights Council has stressed that a lack of accountability by platforms can worsen online human rights abuses.[68] These warnings show why expert views are important to assess the risks of community-driven moderation models. Without local context, crowdsourced moderation often misses harmful subtext and targeted misinformation.

In Bangladesh, civil society groups like Centre for Governance Studies and the Digital Security Forum have raised concerns about Meta's shift.[69] Many claim that Meta rolled out these changes without consultation or local adaptation. And in such a situation, misinformation will only grow without any professional oversight.

Experts suggest that crowdsources moderation can support, but not be reliable for entire content moderation.[70] Especially in complex and polished societies, a hybrid model combining expert review and community input may be the way forward.

2.9. Legal and Policy Frameworks Governing Online Misinformation in Bangladesh

The governance of misinformation and platform accountability in Bangladesh is shaped by a mix of domestic and international legal instruments.

Despite Meta being unregistered in Bangladesh, it cannot avoid local law. In 2024, the government made over 3,700 data requests and Meta compiled most of them.[71] The platform also removed thousands of posts after official complaint.[72] The Bangladesh Telecommunication Act, 2001 gives the Bangladesh Telecommunication Regulatory Commission (BTRC) power to regulate internet services and block content that threatens public order or national security. Meta has previously complied with takedown requests under this framework. This shows that it already operates within the reach of domestic law.[73] Besides, the recently passed Personal Data Protection Ordinance 2025 brings foreign tech firms under Bangladesh court jurisdiction.[74]

It reflects that platforms maintain internal moderation systems but remain accountable

66 Access Now (n 16)

67 Amnesty International, 'Toxic Twitter: Violence and Abuse Against Women Online' <https://www.amnesty.org/en/documents/act30/9260/2018/en/>

68 United Nations Human Rights Council, 'The Promotion and Protection of Human Rights in the Context of Digital Technologies' <https://digitallibrary.un.org/record/3937221>

69 Centre for Governance Studies (n 31)

70 Internews, *Information Ecosystem Assessment – Bangladesh* (Report, March 2024) <https://internews.org/wp-content/uploads/2024/03/IEA-Bangladesh-FINAL.pdf#:~:text=According%20to%20FGDs%20and%20KIIs%20with%20media...and%20disseminating%20relevant%20information%20to%20target%20communities>

71 Transparency Report: Govt sought Meta data on 3,771 accounts in 2024 (Prothom Alo, 13 June 2025)

72 Meta restricts record 2,270 contents in Bangladesh in Jan–Jun (The Business Standard, 5 December 2023) <https://www.tbsnews.net/bangladesh/meta-restricts-record-2270-contents-bangladesh-jan-jun-752366>

73 Bangladesh Telecommunication Act 2001 (BD) ss 30, 55, 97A

74 Mahmudul Hasan and Baharam Khan, 'Shielding personal data: Govt brings big tech under local courts' purview' (*The Daily Star*, 10 October 2025) <https://www.thedailystar.net/news/bangladesh/news/shielding-personal-data-govt-brings-big-tech-under-local-courts-purview-4006206>

to national legal frameworks. In such a situation, Meta's shift from professional fact-checking to Community Notes is not a change within Meta's system. It raises questions about who takes responsibility when harmful content spreads: the company, the volunteers, or the state. Such uncertainty calls for serious consequences especially in Bangladesh where misinformation has already caused violence and harassment.

Besides, the Cyber Security Ordinance 2025 is Bangladesh's current law on online content.[75] It replaced earlier legislation but still relies on broad references to "harmful content." Civil society groups have argued that these clauses remain vague and risk being used selectively.[76] Because of this uncertainty, platforms such as Meta face an unclear legal environment when applying moderation tools like Community Notes.

This domestic framework sits alongside international obligations. Bangladesh is a party to the International Covenant on Civil and Political Rights (ICCPR), which protects freedom of expression under Article 19 while requiring states to prohibit incitement to violence, discrimination, or hostility under Article 20.[77] The Human Rights Committee has clarified that any restriction must be lawful, necessary, and proportionate.[78] These standards are directly relevant to platform governance, as they highlight the need to balance expression with protection from harm.

Beyond law, professional benchmarks provide another point of reference. The IFCN Code of Principles commits fact-checkers to transparency of sources and funding, clear methodology, and open correction policies.[79] While Community Notes is not a professional fact-checking initiative, the IFCN framework offers criteria to judge whether a user-driven system can still achieve neutrality and credibility.

The European Union's Code of Practice on Disinformation (2022) adds a comparative governance model.[80] It requires platforms to cooperate with fact-checkers, provide data access to researchers, ensure transparency in political advertising, and publish detailed moderation reports.[81] Although voluntary and designed for the EU, it sets a standard of accountability that can be used to assess whether Meta applies similar commitments in Bangladesh.

Together, these steps helped build a clear picture of whether Community Notes could work in Bangladesh, especially what strengths it might offer, what risks it carries, and what accountability gaps remain.

75 সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫[Cyber Security Ordinance 2025] (Bangladesh), Extraordinary Gazette, 21 May 2025, Bangladesh Government Press

76 Tech Global Institute & BLAST, 'Joint Statement: Cyber Security Ordinance, 2025 and the Concerns that Remain' (Press Release, 22 May 2025) <https://techglobalinstitute.com/announcements/press-release/joint-statement-cyber-security-ordinance-2025-and-the-concerns-that-remain/>

77 International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) arts 19–20

78 Human Rights Committee, General Comment No 34: Article 19: Freedoms of Opinion and Expression, UN Doc CCPR/C/GC/34 (12 September 2011).

79 Poynter Institute, 'IFCN Code of Principles' (Web Page) <https://ifcncodeofprinciples.poynter.org/>

80 European Commission, '2022 Strengthened Code of Practice on Disinformation' (16 June 2022) <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>

81 European Commission, 'The 2022 Code of Practice on Disinformation' (Policy Page) <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>

3. RESEARCH AIM AND OBJECTIVES

This study aims to explore whether Meta's Community Notes can effectively address misinformation on Facebook in Bangladesh. It focuses on political and gender-based misinformation in a context where digital literacy is still evolving, platform reliance is high, and transparency around moderation is limited.

3.1. Research Objective

1. To assess whether Meta's Community Notes system can effectively mitigate misinformation in a context like Bangladesh, with a specific focus on political and gender-based misinformation.
2. To analyze how digital literacy, language diversity, and narrative dominance influence the effectiveness of user-driven moderation in addressing such content.
3. To suggest ways to improve content moderation practices and strengthen platform accountability in the Bangladeshi context.

4. METHODOLOGY

This study adopted a qualitative approach to explore how Meta's shift to Community Notes might work in Bangladesh. It focuses on understanding the local concerns, risks, and possibilities around this model.

Both primary and secondary data were used. Primary data came from semi-structured interviews with 5 respondents who work closely on misinformation in Bangladesh, for instance- fact-checkers, digital rights experts, and academics. Participants were reached through professional networks using a gatekeeper sampling method to identify those with direct experience.

Each group was asked tailored questions on how misinformation spreads, how current moderation works, and how far platforms like Meta are held accountable. Interviews were conducted online or in person, depending on availability. Verbal or written consent was collected in every case. All interviews were recorded, transcribed, and anonymized when requested. The transcripts were then coded and analyzed thematically.

Secondary data supported these findings. Reports from digital rights groups, academic articles, news coverage, and fact-checking platforms were reviewed to trace how misinformation spreads and how moderation policies have changed over time. Meta's public statements, transparency reports, and relevant laws, including the Cyber Safety Ordinance 2025, Bangladesh Telecommunication Act 2001 were also reviewed to understand the legal scope of platform regulation.

This approach brings together expert views, secondary sources, and international standards. It helps to build a clear picture of how Community Notes might work in Bangladesh. The study looks at both its possible benefits and its limitations. These findings set the ground for a critical discussion in the section below.

5. FINDINGS AND DISCUSSION

This study aims to understand whether Meta's Community Notes can tackle political and gender-based misinformation on Facebook in the Bangladesh context. Selective professionals and academics were interviewed to collect primary data. The findings section shows Community Notes' possible struggle with untrained contributors, language and contextual issues, manipulation risks and so on. It also explores Meta's role in being accountable for such shifts within its platform. The insights from the interviews fit into eight

themes: patterns of misinformation, past moderation, doubts about community notes, risks in a divided society, political and gendered harms, role of civil society and rights groups, gaps in accountability and fixes to make it better. These are elaborated below-

5.1. Understanding the Landscape of Misinformation in Bangladesh

Across the interviews, all participants acknowledged that everyday life within Bangladesh has misinformation that is more common. One participant pointed out the idea that "People often don't even realize they are consuming false content." The participant highlighted that misinformation has become normalized. Notably, Facebook was widely recognized as one of the most powerful platforms to shape narratives. It was used in spreading such content through social media.

There was a shared concern that the rise in misinformation is closely tied to low digital literacy and political polarization. Participants noted that users in the rural areas often lack the tools or resources to question or verify information. One of the participants mentioned, "It's not about being misled intentionally. Sometimes people just don't know how to verify." Participants pointed out that the digital literacy gap creates the fertile ground for misinformation to spread.

The nature of misinformation has also evolved according to the participants. "It was more of a rumor base but recently it is more organized and more related to political narratives." Another added that disinformation campaigns often target women, activists or political leaders. Social media in such cases are used as weapons to target and attack them.

One of the participants mentioned that "Misinformation is embedded in so many ways. For instance, a religious issue is being given a political dimension, a political issue is being given a religious dimension, or a communal issue is being framed with both religious and political dimensions."

Overall, participants agreed that a lack of education on digital tools roots the misinformation ecosystem in Bangladesh. Dominant groups intentionally strategize on how to shape public opinion using social media. The analysis explored how misinformation has evolved from spreading silly rumors to coordinated campaigns over time. Most often, the strategic and coordinated use of misinformation targets political figures and vulnerable groups. It also points out that misinformation is not merely an issue of online space. Rather it is deeply connected with people's beliefs, habits and how they see things. Moderation systems must be capable of understanding where people are coming from or how these narratives spread.

5.2. Reflections on Previous Moderation Practices

Participants shared mixed views in terms of earlier forms of content moderation. Most of them agreed that the partnership with third-party fact checkers was an important step. One participant mentioned, "At least there was some layer of professional filtering." Another referred to the work of fact-checkers as "the silent revolution that was never claimed back." It is because fact-checkers' work has reduced the spread of monetized, sensationalized content from online portals by rating and flagging them as false and incorrect ones. Fact-checkers reduced the reach of monetized or sensationalized content, though they faced threats and bribes from those affected by their ratings.

However, they also highlighted the gaps especially regarding language and cultural context. Fact-checking teams were comparatively small and urban-based. It left out large portions of populations and contents in regional/local dialects. One participant

mentioned, "These variations are difficult to detect or train algorithms to recognize without local assistance." Another participant noted that, "There were too few people trying to do too much" while referring to the large volume of work that needed to be done. While fact-checkers were successful against institutional misinformation, it has "only scratched the surface" in terms of addressing individually spread misinformation according to a participant.

But the participants also mentioned that being a member of the IFCN also required a rigorous review process. The organizations who are members of IFCN have to renew their membership every year upon review. And it keeps the fact-checkers' work impartial and true to its value.

Another common perspective among the respondents was that platforms like Meta did not offer proper infrastructure or long-term support to those partners. One of them pointed out, "They treated fact-checking as an external fix, not an integral part of the platform." This made their efforts like surface-level commitments rather than sustainable solutions.

Despite limitations, participants felt that the fact-checking model offered more accountability and credibility than the model that is being tested now. Because they were trained people, who were at least taken seriously. But the proposed shift would not ensure the same.

5.3. Concerns Around Meta's Shift to Community Notes

The concept of shifting towards community-based moderation elicited a strong reaction from respondents interviewed. Some of them saw potential in decentralizing content moderation but most of them were skeptical about this shift. One of them referred, "Are they professionally trained? How are they going to be held accountable for any action?"

One core concern was the lack of transparency around how contributors are selected and how decisions are made. A respondent noted, "It is a black box" while another mentioned that, "The criteria are very generic requirements that do not in any way, can assess the qualification or the capacity of the person, whether that person can contribute to community notes or not." The requirements to become a contributor which are- being over 18, having a 6-month-old account and having a verified phone number or setting up two-factor authentication are quite generic. These were seen as insufficient to ensure contributor qualifications.

There was also confusion about how this new approach would apply to local contexts like Bangladesh. The model seems disconnected from social, linguistic and political realities of this region and seems to be designed with Western digital culture in mind. One of the respondents mentioned, "You cannot apply US-based solutions to Bangladeshi problems without adapting them as per the context."

Several participants expressed that the shift allows platforms like Meta to wash their hands of responsibility. "Now, if something goes wrong, they can say the community failed, not the platform," mentioned by a participant. It also puts extra pressure on the user base to verify and contribute to a content's authenticity whereas it should be the platform authority's responsibility to do so.

Several participants also felt that the new model demonstrated a significant lack of accountability. They argued that platforms should have independent oversight committees to audit content moderation and ensure that the investment in moderation is proportionate to the amount of content being produced. The reporting system, another content moderation mechanism, also has significant flaws. "They have their reporting mechanisms in place. But they are working

very slowly and need manual review every time someone reports content." The participant also questioned how many are actually getting their grievances redressed, mentioning the numbers as very low.

Instead of strengthening the model of independent fact-checkers with more funding and training, the platform has moved in the opposite direction. As one interviewee mentioned, "I feel like it is a real rollback on what they promised on the path that they were on."

It sums up the concept that the shift to community-based moderation is not just a technical or strategic change. It also changes who is to be held responsible. In countries like Bangladesh where the online space is often misused, most of them felt that the shift might neither be a smart move nor a safe decision.

5.4. Community Moderation and Its Risk in a Polarized Context

Nearly all the participants highlighted that community-based moderation may be harmful in a polarized society like Bangladesh. The risk of coordinated manipulation was also a common concern among the participants. One of the respondents asked, "In a place where political groups are already so active online, what stops them from dominating the community notes process?" They worried that groups with strong political feelings could easily take over the process to push their own agenda. As one of them explained, "partisanship can be the main force behind political misinformation, while group affiliation in terms of religion can reinforce religious misinformation." This means the system would be trying to work in a society where people already have strong beliefs that lead them to trust certain information and ignore other information. It makes it very easy for biased groups to manipulate the system and silence others.

Another interviewee highlighted that online spaces are often used to oppress the voice of minor groups. A respondent mentioned, "Minority voices, political opposition, and feminists are already targets in the online space. Now you're letting anyone decide what counts as truth? Do they expect all the people on the internet to possess a liberal mindset to accommodate their opinions and thoughts all of a sudden?" This is particularly concerning for minorities, as a majoritarian system will never let them win against their views.

They also mentioned that Community Notes being the content moderation system, will not restrict the continuous spread of a piece of information. One of them added, "Community Notes does not restrict the circulation of flagged content, rather it keeps the risk of initiating violence alive. And we all know that such riots or violence are spread like wildfire on social media."

The lack of protection for marginalized groups was a common concern among the participants. They mentioned that harmful narratives around women and ethnic and religious minorities can go unchecked without professional oversight or proper training. One of them responded, "Who will be the new gatekeepers of content, and what qualifications will they need for this role? You can't simply rely on, say, an engineer for a kidney transplant." Another participant responded, "Community moderation assumes neutrality, but in Bangladesh, neutrality is hard to find online." Participants also gave specific examples of how online misinformation campaigns led to offline harmful actions. For instance, extremists being mobilized using social media to attack and kill bloggers on earlier years or get a perpetrator of sexual abuse against a woman released from police custody.

There was also doubt about the responsiveness of the system. Participants

noted that fact-checking was difficult, even when they had a timeline. They had to respond to a query within 24-48 hours to a requested review. Few of the participants also raised concern regarding the time-consuming process of the visibility of Community Notes. One of them referred to it as a "slow response system" when it comes to taking prompt action to prevent any violence or riot. But community notes can take days or weeks, if at all, to appear. "By the time a correction comes, the damage is already done," one participant said.

5.5. Political and Gendered Dimension of Misinformation

One of the participants mentioned that, "Misinformation in these regions has always been used as a tool of political advantage." They are particularly spread around elections where opposition voices are silenced through targeted campaigns.

Another participant pointed out while discussing gender that "Women are often disproportionately targeted by misinformation." Especially women in politics, journalism and activism frequently face online abuse tied to their personal lives, relationships or morality. These narratives often expose them to real life threats. Participants noted that such content is rarely flagged or removed under current moderation rules. They also added that it becomes really tough when hate is spread through voice cloning or posts being shared as opinions, not facts. Then it becomes tough even for the trained moderation team to flag them. Discussing this, they shared concern about untrained contributors who can barely flag those contents by identifying them.

There was also concern about how the new moderation system (Community Notes) can fail to recognize the nuance in gendered misinformation. A major concern was that Meta's initial content moderation policies were 'Western-centric'. They did not account for local contexts, such as hate speech targeting specific ethnic and religious groups. This highlights a significant concern that a community-based system will similarly struggle to address these complex issues. As one of the participants explained, "We really had to struggle to get Meta to recognize the existence of hate speech in Bangladesh and to hire local moderators who understood the language and context." This demonstrates how algorithmic and community-based models risk amplifying rather than challenging pre-existing gendered power dynamics in the online space.

5.6. Power, Participation and the Role of Civil Society

All interviewees expressed that power in the digital space is asymmetrical. This pattern is observed within the broader civil society ecosystem as well. According to one of them, civil society, the leftist-liberal group of people, may have their impact over social media but eventually they will be cornered by the fundamentalist, centrist group of people. The participant also noted that "Bangladeshi civil society has had very limited say in how moderation frameworks are designed or rolled out." It took a long time and a real "struggle" for civil society to get Meta to even acknowledge specific kinds of hate speech and hire local moderators who actually understood the language and context.

This lack of participation has implications for trust and legitimacy. Civil society groups that have long worked to promote digital literacy and combat online abuse now find themselves sidelined. Participants suggested that the shift represents a broader move towards platform self-interest, where decisions are driven by PR optics and operational cost-cutting rather than user safety or public interest. One interviewee said that this new model is a "complete rollback on what they promised" and a way for platforms to "wash their hands of responsibility."

However, participants also highlighted that coordinated efforts from these groups are necessary to ensure accountability from platforms. One participant mentioned that, "There is a lack of joint efforts of Bangladeshi activists at the global level. It can be due to the fewer number of digital rights activists from our country. But it is very much needed to ensure accountability from the platforms." Another participant mentioned that it is also important for rights activists to work as a pressure group on the government, putting "Emphasis on the government to enact such laws and policies that hold such platforms accountable." This suggests that while civil society has been left out, a coordinated approach is seen as essential for compelling both platforms and the state to take responsibility.

5.7. Platform Accountability during the Changed Content Moderation System

Participants shared several interlinked opinions in terms of what platform accountability should look like. Most of them marked that accountability is not confined among legal standards but it also lies within moral and social responsibility to protect vulnerable users. One of them stated, "Platforms like Meta must take responsibility for the impact of contents that are posted here."

Participants also criticized Meta's community driven moderation being a way to "shift to blame the users" rather than investing in systematic change. As one of them stated, "They announced replacing professionals with volunteers and told the world it was democracy." The participants argued that real accountability is ensured when local voices are included in creating rules along with regular, rigorous systems of addressing feedback. One of them said, "Accountability is when people affected by the rules also help shape them." Most participants felt that Meta's current actions fall short of this standard.

At present, most participants felt that Meta's actions fall short of this standard. From a broader perspective, they also voiced concerns about the long-term effects of this new model. One of the respondents said, "It can result in decreased trust among users, digital disengagement, and platform switching could be potential results, altering how they experience Meta's platforms."

5.8. Legal and Policy Implications of Community Notes

The selective legal and policy frameworks analyses show clear challenges for Community Notes in Bangladesh. The Cyber Security Ordinance 2025 regulates "harmful" online content, but its language is broad and vague. This leaves platforms like Meta uncertain about what counts as misinformation. Shifting moderation to users, as Community Notes does, could worsen this problem, especially for women and minorities who are already vulnerable.

International standards, such as the ICCPR, stress that freedom of expression must be balanced with preventing violence, discrimination, or hostility. Your findings suggest that volunteer contributors may not recognize politically or socially sensitive content. This means harmful posts could stay online, putting people at risk.

Professional benchmarks like the IFCN Code of Principles and the EU Code of Practice on Disinformation stress transparency, accountability, and structured verification. Community Notes currently lacks these safeguards. Contributors are untrained, decision-making is unregulated, and responses are slow, making it hard to prevent the spread of misinformation effectively.

Overall, applying these frameworks shows that Community Notes does not fully meet the standards set by law, international human rights obligations, or professional best

practices. Without these safeguards, the platform risks allowing misinformation to spread and shifting responsibility away from those who control the platform.

5.9. Ways to Improve Meta's Content Moderation: Considering Meta as a Case Study

Respondents' insights were practical and contextualized in terms of suggesting moderation strategies. Their responses reflected a desire for hybrid and inclusive strategies, drawing on grounded, context-specific insights.

One of the primary recommendations was to strengthen local fact-checkers instead of discarding this model in the near future. As one of them mentioned, "Invest in their growth instead of discarding them." They felt that professional oversight is a key part of the solution and it should be improved with time.

Another respondent suggested a 'hybrid model.' This would combine community feedback with professional oversight. The participant also added that "crowdsourcing alone cannot work in countries with political polarization and limited digital literacy." This approach would balance both the scale of the community and the expertise of professionals.

The need for better language support was also a major point. One respondent stressed, "You can't moderate what you don't understand." They urged platforms to hire teams with cultural and linguistic expertise in local dialects such as Sylheti and Rangpuri. This would ensure that content in these languages doesn't go unchecked.

Finally, some respondents argued that accountability should be written into law. They proposed updating Bangladesh's legal framework to require platforms to be transparent and to consult with the public. This would provide external pressure to ensure companies prioritize user safety.

6. RECOMMENDATIONS AND CONCLUSION

This research explored whether Meta's Community Notes can effectively address political and gender-based misinformation in Bangladesh. The data show that while the idea of a community-based system may seem democratic, its use in Bangladesh might have some serious implications.

Experts and digital rights professionals shared similar concerns. They expressed concerns about untrained volunteers, the risk of political groups taking over, and a lack of transparency. At the same time, they offered practical ideas that are rooted in the realities of Bangladesh.

The main recommendations from this study are set out as follows:

- Meta should reinstate and reinforce existing fact-checking and content moderation teams involving professional fact-checkers who have both local knowledge and insights and the expertise required to verify the authenticity and accuracy of information.
- Meta should develop a hybrid moderation model combining community participation with oversight from trained moderators, so as to balance community inclusion with credibility and integrity of information.
- Meta should expand on existing language and dialect moderation processes, including building in understanding and coverage of local dialects and linguistic and cultural nuances, especially in underserved areas and among marginalized communities.
- Ensure transparency about the selection of community contributors and decision-making regarding moderation.

- Meta should engage with local civil society and rights organizations to shape, review, and create platform policies.
- States should develop legal frameworks requiring regular audits and local consultations to ensure platform accountability, drawing inspiration from instruments like the EU's Digital Services Act.

In conclusion, Meta's current community-driven model is not ready for the complex challenges of Bangladesh. Without major changes, it risks ignoring vulnerable voices and allowing misinformation to spread unchecked. The platform must move beyond symbolic shifts. It needs to invest in real strategies that prioritize safety, inclusiveness, and accountability. For content moderation to work in Bangladesh, it must be shaped by the people who face the consequences of misinformation.

CHALLENGES IN ACCESSING JUSTICE

Tech Facilitated Gender-based Violence in Bangladesh

Saraban Tahura Zaman

Abstract

Incidents of Technology Facilitated Gender-based Violence (TFGBV) are rising at an alarming rate in Bangladesh, posing multifaceted threats to women. An increase in digital footprints left by internet users, lack of digital literacy, and a lack of understanding about digital communication ethics are some major reasons behind this rise. Nevertheless, justice for survivors of such violence often remains out of reach. Against this background, this research investigates gaps within the Bangladesh legal system which prevent complainants of TFGBV from accessing justice. Drawing from both doctrinal analyses and empirical evidence from semi structured interviews conducted with key stakeholders, this research finds that inadequate legislative measures to protect women from TFGBV, difficulty in filing complaints, inadequate framework on handling digital forensic evidence, and the lack of capacity of legal aid service providers to respond to the needs of TFGBV complainants from marginalized communities serve as the major challenges in finding justice. Based on these findings, the research makes recommendations to specific stakeholders to mitigate these

Keywords: *TFGBV, Access to Justice, Complaint Mechanism, Digital Evidence.*

1. INTRODUCTION

The United Nations Population Fund (UNFPA) defines Technology-Facilitated Gender-based Violence (TFGBV) as "*an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media against a person on the basis of gender.*"[1] It includes, among others, harassment, image-based abuse, stalking, blackmail, revenge porn, extortion including sextortion, doxing, impersonation, hate speech, defamation, and using technology to locate women to perpetrate violence.[2] Advancements in AI technologies have opened up newer avenues of harassment for women online, such as non-consensual sexual image and video generation.[3] Perpetrators of TFGBV may be motivated by revenge, jealousy, political agenda, ideological agenda, sexual desire, or monetary need.[4]

Bangladesh has also seen a recent increase in incidents of TFGBV, requiring much-deserved attention. A study conducted in 2024 by NETZ Bangladesh found that over 78% of women in Bangladesh face TFGBV.[5] 78.4% of these incidents occurred on Facebook, while 28% were committed through various messaging apps like WhatsApp and IMO. The severity of the incidents varies from case to case. Severe cases are sometimes reported, whilst a majority of the cases, severe or less severe, go unnoticed. While these incidents are clearly on the rise, Bangladesh Mahila Parishad's report on violence against women and girls through January to June 2025 shows only 11 reported incidents of cybercrime.[6] The 2014-15 Report of the Web Index reveals that in 74% of the Web Index countries, meaning 64 out of 86 countries including Bangladesh, law enforcement agencies and courts are failing to take appropriate measures to address TFGBV incidents.[7] Although the legal framework around cyber protection in Bangladesh has evolved through a series of enactments and repeals in recent years, meaningful accountability often remains elusive. Out of 40,280 cybercrime complaints received by the Police Cyber Support for Women (PCSW) between 2020 and 2024, 15,895 complainants chose not to pursue legal action and withdrew their complaints even after PCSW had completed initial investigations and arrested suspects. In the Dhaka Cyber Tribunal, only 213 verdicts were delivered out of 2,141 cases between 2014 and 2022, with 162 acquittals; these indicate that very few victims actually see justice.[8] It is therefore necessary to identify the issues in the legal system that prevent victims from seeking and finding justice. For the

1 UNFPA, *What is technology-facilitated gender-based violence?* (Brochure, March 2023) https://www.unfpa.org/sites/default/files/resource-pdf/TFGBV_Brochure-1000x560.pdf.

2 ibid.

3 Suzie Dunn, 'Identity Manipulation: Responding to Advances in Artificial Intelligence and Robotics' (Paper delivered at We Robot 2020, Ottawa, May 2020) https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1776&context=scholarly_works.

4 Laura Hinson et al, *Technology-Facilitated Gender-Based Violence: What Is It, And How Do We Measure It?* (ICRW Brief) https://www.icrw.org/wp-content/uploads/2018/07/ICRW_TFGBVMarketing_Brief_v8-Web.pdf.

5 Staff Correspondent, 'Over 78pc women face tech-based violence in Bangladesh' *The Daily Star* (online, 12 December 2024) https://www.thedailystar.net/news/bangladesh/news/over-78pc-women-face-tech-based-violence-bangladesh-3774116.

6 Bangladesh Mahila Parishad, *VAWG Chart* [January – June, 2025] (Report, 1 July 2025) https://mahilaparishad.org/vawg/vawg-chart-january-june-2025/).

7 World Wide Web Foundation, *WEBINDEX Report* 2014-15 (Report, 11 December 2014) https://thewebindex.org/wp-content/uploads/2014/12/Web_Index_24pp_November2014.pdf.

8 Mohammad Jamil Khan & Emrul Hasan Bappi, 'Cybercrimes continue to scourge women' *The Daily Star* (online, 3 November 2024) https://www.thedailystar.net/news/bangladesh/crime-justice/news/cybercrimes-continue-scourge-women-3743096.

purpose of this research, the 'legal system' would include legislative measures, complaint mechanisms, investigation and trial processes, and legal aid services.

2. METHODOLOGY

This research adopts a mixed-method qualitative approach, combining doctrinal legal analysis with qualitative empirical research. The doctrinal analysis involves a reading of key provisions in the *Cyber Security Ordinance 2025, Penal Code 1860, Women and Children Repression Prevention Act 2010*, and *Legal Aid Services Act 2000*. Statutes, case law, and scholarly commentary are the sources of data used for this section of the paper. The empirical component draws insights from four Key Informant Interviews (KIIs) with key stakeholders: 1 Judicial Magistrate, 1 civil society representative, and 2 Advocates. Interviews were conducted between April-June 2025, guided by a semi-structured questionnaire designed to elicit perspectives and experiences on existing issues in the legal system that pose challenges for complainants of TFGBV seeking legal redress. The interviewees were selected using purposive sampling, focusing on individuals with direct involvement in or knowledge of the legal system of Bangladesh, and hands-on experience with matters relating to TFGBV. All participants were informed about the purpose of the research and consent was obtained.

3. FINDINGS AND DISCUSSION

3.1 Scattered Laws, Inadequate Protection

While some forms of TFGBV fit into the definitions of various criminal offences outlined in the penal and criminal laws of Bangladesh, none of the laws explicitly define TFGBV. More importantly, not all forms of TFGBV are considered a crime under the Bangladeshi legal framework. *The Women and Children Repression Prevention Act 2000* provides a very constrained definition of sexual abuse in section 10, requiring the victim to be physically touched by the perpetrator.[9] Subsequently, section 2(1)(za) of the *Cyber Security Ordinance 2025* broadened the scope of protection for sexual abuse on the internet, by including repeated demands for nude images, misuse of authority to propose illicit relations, sending sexually explicit or pornographic content without consent, digitally sexualizing someone's image, or making threats and inducements to coerce sexual relations as part of the definition of sexual harassment.[10] Section 2(1)(ra) defines 'revenge porn' as the non-consensual dissemination of a person's intimate or private images or data with the intent to cause harm.[11] T*he Cyber Security Ordinance 2025* also criminalizes sextortion, and image or video-based abuse through the use of Artificial Intelligence (AI) technology.[12]

These definitions still do not encompass all forms of sexual harassment that may occur, particularly in online spaces. The judgment of the High Court Division of the Supreme Court of Bangladesh in *Bangladesh National Women Lawyers' Association (BNWLA) v Bangladesh*, delivered in 2011 (expanding upon the landmark ruling of 2009),[13] had provided a more comprehensive definition of sexual harassment, which was made applicable only to work places and educational institutions, with directives upon lawmakers to formulate specific laws to counter sexual harassment.[14]

9 *Women and Children Repression Prevention Act* 2000 s 10.
10 *Cyber Security Ordinance 2025* s 2(1)(za)
11 *Cyber Security Ordinant 2025* s 2(1)(ra)
12 *Cyber Security Ordinant 2025* s 25
13 14 BLC (2009), 694
14 18 BLC (2013) 290.

The enactment of the *Cyber Security Ordinance 2025* was the ideal occasion to act upon the High Court directives, and provide an all-encompassing and expansive definition of sexual harassment, covering incidents occurring in the cyber space. The opportunity, however, was left unutilized.

The *Pornography Control Act 2012* penalizes the production of pornography; forcing, coercing, or enticing women, men, or children to participate in it; recording their images or videos with or without consent; using pornography to damage a person's social or personal reputation; extorting money or other advantages through threats or intimidation involving pornography; subjecting someone to psychological abuse by exploiting pornographic material; and distributing or supplying pornography via the internet, mobile phones, or other electronic devices.[15] These encompass acts of image based abuse, blackmail, extortion, and sextortion.

Doxing, impersonation, hate speech, and stalking are some forms of TFGBV that do not on their own constitute a crime under the Bangladesh legal framework. Doxing is the act of publishing private personal information.[16] *The Personal Data Protection Ordinance 2025 (Draft)* is not intended to protect personal information disclosed at a personal capacity, and thus, does not aim to provide protection against doxing. Impersonation must be used to commit cheating in order to constitute a crime,[17] and therefore does not include the creation of fake social media accounts or other modes of online impersonation to harass women. Stalking is recognized as a form of sexual harassment under the High Court's directives in *BNWLA v Bangladesh*, which are legally binding and enforceable until a formal legislation is enacted, but Acts of Parliament are yet to recognize this as a criminal offence, in either offline or online contexts. Physical violence perpetrated through the use of technology may form various degrees of crime (i.e. hurt, grievous hurt, rape, murder).[18]

While these are some common forms of TFGBV, it can manifest in various other ways which, in most cases, are not specifically criminalized in Bangladesh. Even types of TFGBV that are legally recognized as crimes are dispersed across different laws, often subject to varying procedures for survivors seeking redress, highlighting a lack of uniformity in application, and creating obstacles in their pathways to justice.

3.2 The Complaint Mechanisms are Ineffective

TFGBV survivors have to choose between multiple options to initiate legal proceedings, which often is the reason for confusion and deterrence from initiating legal action. In cases where the offense is non-cognizable, the complainant is required to register a General Diary (GD) entry; conversely, for cognizable offenses, a First Information Report (FIR) must be filed.[19] Both procedures are to be executed at a police station. In instances where police refuse to record a GD/FIR,[20] complaints can be filed directly before a Judicial Magistrate. If the offense constitutes a crime under the *Cyber Security Ordinance 2025,* the complaint appears before the Cyber Tribunal, provided that the complainant swears an

15 *Pornography Control Act* 2012 (Act No IX of 2012), s 8.

16 UNFPA, 'Technology-Facilitated Gender-Based Violence: A Growing Threat' (Web Page) https://www.unfpa.org/TFGBV.

17 *Cyber Security Ordinant 2025* s 23; Penal Code 1860 s 416.

18 *Penal Code 1860* ss 319, 320, 300, 375.

19 *Code of Criminal Procedure 1898* s 154; Police Act 1861 s 44.

20 Md Ariful Islam, 'Cyber law gaps fail to shield victims of AI-driven abuses' *The Business Standard* (online, 4 August 2025) https://www.tbsnews.net/bangladesh/crime/cyber-law-gaps-fail-shield-victims-ai-driven-abuses-1203876.

affidavit attesting to the police station's unwillingness to record the GD/FIR.[21] Complaints can also be filed online to the CID's Cyber Police Center, or Police Cyber Support for Women (PCSW).[22] To this end, one of the Advocates of the Supreme Court noted,

"*The general public does not have proper understanding or knowledge about how legal complaint mechanisms work. The victims of TFGBV are already traumatized and lack immediate access to support mechanisms that enable them to make informed decisions about their next course of action in terms of filing a case or complaint. Additionally, legal language is not easily comprehensible to the general public. Therefore, victims' decision to take legal advice and or filing complaints gets delayed*."

The civil society representative interviewed echoed these observations:

"*A major concern for TFGBV victims is figuring out where and how to file the complaints. Even I do not have adequate information about the process to follow, if I face cyber harassment or threats as such. There is information available online, but I find it very scattered and not well coordinated*."

Lack of uniformity in the application of laws and legal procedures is compounded by challenges in filing complaints, which only serves to deter complainants from pursuing legal action against perpetrators and seeking justice.

3.3 Capacity to Handle Digital Evidence and Forensics is Deficient

The low rate of conviction in cases before the Cyber Crime Tribunal is largely due to inadequacy of evidentiary support. In cases of TFGBV, digital evidence is very sensitive in nature and there is always a risk of such evidence being leaked or altered, which may lead to further abuse. It is therefore of utmost importance to strictly adhere to the procedures of handling digital evidence. Handling of digital evidence includes identification, collection, acquisition and preservation of potential digital evidence.[23] Maintaining a chain of custody record, i.e. a document identifying the chronology of the movements and handling of the potential evidence is an essential condition for admissibility of any digital evidence as per the international standards.[24] The *Cyber Security Ordinance 2025* provides for the operation of digital forensic labs for the fulfilment of the Ordinance's purposes.[25] Section 11(2)(e) mandates that the forensic labs will carry out their functions in accordance with scientific procedures and in the manner prescribed by rules.[26] Rules under the *Cyber Security Ordinance 2025* have not yet been formulated. The draft rules under the now repealed *Cyber Security Act 2023*, proposed in 2024, were in large part a verbatim reproduction of the *Digital Security Rules 2020*.[27] Both sets of rules attracted extensive criticism, particularly with respect to the provisions on digital forensics. Neither incorporated internationally recognized ISO

21 *Cyber Security Ordinant 2025* s 40.

22 Mohammad Jamil Khan, 'Rising Cybercrime: Police hotlines flooded with complaints' *The Daily Star* (online, 23 December 2020) https://www.thedailystar.net/frontpage/news/rising-cybercrime-police-hotlines-flooded-complaints-2015589.

23 International Organization for Standardization, *Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence* (ISO/IEC 27037, 15 October 2012) 8.

24 ibid, 10.

25 *Cyber Security Ordinant 2025* s 10(1).

26 *Cyber Security Ordinant 2025* s 11(2)(e).

27 Quazi MH Supan, *Review of Proposed Cyber Secuirty Rules, 2024* (Position Paper, 13 June 2024) https://www.ti-bangladesh.org/upload/files/position-paper/2024/pcsr/Review-of-proposed-Cyber-Security-Rules-2024-En.pdf 7.

standards for the handling of digital evidence.[28] With the emergence of newer technologies, including AI-based capacities, it is imperative that the forthcoming rules under the 2025 Ordinance ensure the highest possible standards in this regard. Until such rules are enacted, the standards remain undefined, which contributes significantly to the persistently low rate of conviction in TFGBV cases that proceed to trial. According to one of the advocates who participated in the study,

"*There is no scope in the laws or in the process where the principles and ethics of maintaining digital evidence are stipulated clearly, when it is one of the most important factors in deciding cases of cybercrimes, especially TFGBV. If any information is leaked or tampered with, then not only will justice for the victim be jeopardized, the safety and security of the victim/complainant will also be compromised*".

The infrastructure for preserving digital evidence is undeveloped. As per the interviewees, neither the courts nor the police stations are adequately prepared to manage digital evidence. Instances of evidence becoming corrupt, or being lost, are also not rare. This was echoed by the Judicial Magistrate interviewed, who stated,

"There is no digital forensic lab anywhere in Bangladesh attached to the court or police stations. Digital evidence saved in CDs or in memory cards or pen drives are always attached to the 'Case Nothi' (case documents), which are generally stored in a 'malkhana' (evidence room). And a number of times, this evidence is either lost, damaged or at risk of being tampered with. Even police stations do not have proper storage facilities at divisional or district level to store digital evidence and maintain the digital chain of custody with utmost care. Evidence management system is a key part of the criminal justice system and absence as such may lead to evidentiary weakness. There is no digital forensic Lab in Bangladesh at district level. Therefore, it takes a long time to cross check any digital evidence when required."

Handling and using digital evidence require a certain extent of technical knowledge. In cases of TFGBV, it is crucial that the Investigation Officers (IO) are technically knowledgeable, well trained, and equipped to conduct such investigations. However, the scope and opportunity for their training is insufficient. The Cyber Police Center (CPC) is a training initiative by the CID to build the expertise of officers on cybercrime, cyber security and digital forensics.[29] Since its inauguration in 2017, it has only been able to train 600 individuals.[30] Capacity building opportunities for court staff, evidence room staff, and even judges, are scant, as per the Judicial Magistrate interviewed. To effectively adjudicate cases of TFGBV, he urged for appropriate digital forensic equipment and courtroom facilities.

3.4 Legal Aid Services are Inadequate

The *Legal Aid Services Act 2000* has established legal aid committees in each district of Bangladesh to ensure justice for people who cannot afford legal support.[31] An eligible person can receive legal assistance from the government legal aid mechanism free of cost. Panel lawyers who provide this assistance are selected by their respective District Legal Aid Committees, and the Supreme Court Committee formed under the Act.[32] Lawyers empaneled under the government-funded legal aid

28 ibid 13.
29 'Cyber Police Center' *CID* (Web Page) https://www.cid.gov.bd/cpc.
30 ibid.
31 *Legal Aid Services Act 2000.*
32 *Legal Aid Services Act 2000* s 15(2).

program often lack the requisite competence and commitment to effectively handle complex and sensitive cases, including those involving TFGBV.[33] The selection process overlooks specialization and does not ensure sufficient training, leading to the appointment of underqualified and/or politically affiliated lawyers who frequently deliver services in a cursory or insincere manner.[34] Moreover, inadequate monitoring, poor remuneration, and the absence of accountability mechanisms further erode the quality of legal representation provided to vulnerable clients.[35] Women survivors of sexual violence, including TFGBV, may prefer to seek help from women lawyers.[36] Though the Act provides for one third of the selected panel lawyers to be women,[37] this is not mandatory "(at least one woman lawyer, *if found*, shall be included"), which enables the provision to be ignored in practice. All these factors combined deter TFGBV victims in marginalized communities from seeking justice through the legal aid office. Even when they seek help, inadequate technical capacity contributes to a lesser success rate in attaining justice.

Several NGOs, including Ain o Salish Kendra (ASK), Bangladesh Legal Aid and Services Trust (BLAST), Bangladesh Mahila Parishad, Naripokkho, and Bangladesh National Women Lawyer's Association (BNWLA) offer legal aid services for TFGBV victims.[38] However, the fact that almost 90% of instances of online violence go unreported[39] shows that besides offering legal aid services, both government legal aid offices and NGOs must proactively promote their services, engage in outreach activities, and ensure visibility within target communities to bridge the existing gap between availability and accessibility.

The Multi-Sectoral Program on Violence Against Women (MSPVAW), implemented by the Ministry of Women and Children Affairs, has established 14 One Stop Crisis Centers (OCCs) at various Medical College Hospitals around the country.[40] OCCs provide comprehensive, centralized support to women survivors of violence, including police support, healthcare, legal aid, and counseling. The operation of the OCCs is however limited to physical violence.[41] TFGBV cases that do not subsequently escalate to physical violence are currently not covered within the scope of OCC services. A comprehensive support framework is, therefore, essential for all TFGBV survivors and complainants, both to provide immediate care and to facilitate access to justice. Lack thereof contributes significantly towards failure to ensure justice in many TFGBV cases.

4. RECOMMENDATIONS

I. Fixing the issue of scattered laws, directives, and ordinances would require repeal of several provisions, and enacting a unified law encompassing all

33 Farzana Akter, 'Legal Aid for Ensuring Access to Justice in Bangladesh: A Paradox?' (2017) *Asian Journal of Law and Society* 4(1) 1-19.

34 ibid.

35 ibid.

36 Jamila A Chowdhury, 'Weighing the Gender Hypothesis on Mediators: Insiders' View from District Legal Aid Offices in Bangladesh' (2021) *Dhaka University Law Journal* 32(2), 69, 81.

37 *Legal Aid Services Act 2000* s 15(3)

38 Bangladesh Legal Aid and Services Trust, *Legal Action On Cyber Violence Against Women* (Report, December 2017) https://www.blast.org.bd/content/publications/Cyber-violence.pdf.

39 Farhana Akter, 'Cyber violence against women: the case of Bangladesh' GENDER IT (Web Report, 17 June 2018) https://genderit.org/articles/cyber-violence-against-women-case-bangladesh.

40 Nilima Jahan, 'One-stop crisis centre: Conviction in less than 2pc cases', The Daily Star (Online, 02 November 2024) https://www.thedailystar.net/news/bangladesh/crime-justice/news/one-stop-crisis-centre-conviction-less-2pc-cases-3742446.

41 ibid.

forms of gender-based violence. While that may not be feasible, since different laws have different purposes, both victims and legal actors would benefit significantly from the systematic dissemination of consolidated information on TFGBV and its related offence.

II. Legislative reforms are needed to criminalize forms of TFGBV that remain unaddressed under existing Bangladeshi law. In this regard, the directives issued by the High Court in the *BNWLA* judgment should be implemented without delay.

III. Systematic dissemination of information about available complaint mechanisms, such as the process of reporting a GD or FIR, seeking help from PCSW, Legal Aid offices, OCCs, and relevant NGOs is essential. The government and law enforcement agencies must collaborate to ensure their effective implementation, while also taking steps to streamline these mechanisms for greater accessibility and efficiency.

IV. Specialized training programs must be institutionalized within the justice sector to build the technical capacity of justice sector actors to handle digital evidence and digital forensics, with such initiatives needing to be expanded across the judiciary, prosecution, and law enforcement agencies. Clear procedural rules should be enacted in line with the *Cyber Security Ordinance* to govern the collection, preservation, analysis, and admissibility of digital evidence. Additionally, investment is needed to establish and maintain secure, standardized digital evidence storage facilities to ensure integrity, chain of custody, and compliance with evidentiary standards.

V. Capacities of government legal aid services and service providers must be enhanced across all levels to strengthen access to justice for TFGBV survivors. Legal Aid Committees should prioritize empaneling lawyers with expertise in handling cases with digital evidence, while also ensuring greater representation of women to create a more supportive environment for survivors. Public outreach efforts must be intensified so that marginalized and low-income survivors are aware of their right to free legal assistance and are encouraged to seek redress.

CYBER PROTECTION ORDINANCE 2025 AND THE POLITICS OF CONSENT

Rethinking Online Intimacy, Gender, and Law in Bangladesh

Tabassum Nuha

Abstract

This paper critically examines Section 25 of the Cyber Protection Ordinance 2025 in Bangladesh, which criminalizes the non-consensual sharing of intimate imagery (NCII) content. The provision acknowledges the issue of online gender-based violence, including 'revenge pornography'. It does not clearly define the framework for 'consent', which may lead to moral surveillance instead of actual digital justice. The study has been conducted from a feminist perspective. The paper argues that Section 25 adopts the 'women as victim' concept, undermining their agency. This provision also fails to provide any special protection for Hijra community members and people with other diverse and non-conforming gender identities. In effect, it often leaves out marginalized communities. This happens because the law does not recognize queer romantic and/or sexual relationships outside of heteronormative couple-hood, so their complaints may be dismissed. In exploring the impact of Ordinance provisions on marginalized identities, the study explores perspectives from other South Asian countries, where laws similarly tend to prioritize moral regulation over rights-based digital protection. The study concludes with recommendations for legal and policy changes that focus on redefining terms and ensuring overall gender inclusivity in Bangladesh.

Keywords: *Cyber Protection Ordinance 2025, NCII, Revenge Pornography, Gender, Bangladesh*

1. INTRODUCTION

In recent years, the rapid expansion of digital communication has intensified both opportunities and vulnerabilities for expression, particularly for women and marginalized communities navigating online spaces.[1] Across South Asia, the legal landscape governing cybercrime and digital sexuality has often struggled to keep pace with evolving social and technological realities.[2] This gap is evident in how online gender-based violence (GBV), such as non-consensual image sharing, doxxing, or digital harassment, is often not properly addressed. Instead of focusing on protecting consent and safety, the laws focus more on controlling people's behavior and ideas about morality. Bangladesh's Cyber Protection Ordinance 2025 is the latest legislative attempt to address online harm as an alternative to the widely condemned Cyber Security Act 2023.[3] Civil society groups, journalists, and human rights activists have criticized the earlier law for retaining overly broad and repressive provisions.[4] Among the newly introduced Ordinance's provisions, section 25 is significant as it criminalizes the non-consensual distribution, or the threat of such distribution, of intimate content.[5] It seeks to address the concerning increase in online abuse, such as deepfakes, revenge porn, and image-based abuse, particularly against women and children. However, despite its protective ambitions, Section 25 raises important concerns about how consent, gender, and digital intimacy are constructed within the law.

Although the ordinance aims to introduce new types of online harm, it remains limited by traditional constraints and lacks a clear legal definition. It also reflects a regional trend of regulating bodies through moral perspectives. Because of religious, social, and cultural values, section 25 effectively excludes the agency of transgender and non-binary individuals. This raises the following questions: Whose consent does the law recognize? Who is assumed to need protection, and who is ignored, erased, or punished? This study has sought to explore feminist legal theory[6] and literature highlighting South Asian regional perspectives to understand and answer these questions. It also provides a close reading and critique of Section 25, highlighting its conceptual and procedural gaps. It finally observes that legal frameworks often reinforce patriarchal norms under the guise of ensuring protection for women and children.[7]

1 'Online and ICT-Facilitated Violence against Women and Girls during COVID-19', *UN Women – Europe and Central Asia* (2020) <https://eca.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19-1>.

2 'Digital-Governance-and-Rights-in-South-Asia-and-the-Path-Forward.Pdf' <https://techglobalinstitute.com/wp-content/uploads/2025/02/Digital-Governance-and-Rights-in-South-Asia-and-the-Path-Forward.pdf>.

3 Legal Giant, 'Cyber Security Ordinance 2025: Is It Better or Worse?', *Legal Giant Bangladesh* (22 May 2025) <https://legalgiantbd.com/cyber-security-ordinance-2025-is-it-better-or-worse/> ('Cyber Security Ordinance 2025').

4 'Govt Decides to Repeal Cyber Security Act', *The Business Standard* (7 November 2024) <https://www.tbsnews.net/bangladesh/interim-govt-decides-repeal-cyber-security-act-987236>.

5 Cyber Security Ordinance 2025, s 25.

6 Robin L West, 'Women in the Legal Academy: A Brief History of Feminist Legal Theory' (SSRN Scholarly Paper No 3300343, Social Science Research Network, 12 December 2018) <https://papers.ssrn.com/abstract=3300343> ('Women in the Legal Academy').

7 'EROTICS South Asia Exploratory Research: Sex, Rights and the Internet' <https://www.apc.org/sites/default/files/Erotics_1_FIND.pdf>.

2. WHY A NEW LAW?

When examining the legislative rationale for Section 25, it is essential to understand why Bangladesh opted to introduce a new ordinance rather than amend existing laws. Current laws addressing sexual violence, especially gender-based online violence, are outdated. They are fragmented, as legal protections related to consent, privacy, and online harm are scattered across multiple disconnected laws. For instance, the Nari O Shishu Nirajatan Daman Ain, 2000,[8] is a key legislation concerning acid violence, trafficking, rape, and sexual assault under Sections 4, 5, 9, and 10. However, neither the 2000 Act, nor its latest amendment, the Nari O Shishu Nirjatan Daman (Amendment) Ain, 2020,[9] addresses cyberviolence; the legislation has not been updated to build in protection against emerging forms of gender-based violence, like non-consensual intimate imagery (NCII) or stalking in online environments. The Pornography Control Act, 2012, also criminalizes the production, possession, and distribution of pornography in Section 8 without distinguishing between consensual and non-consensual content. The law conflates "immoral" material with harm and fails to consider the victim's agency, consent, or privacy concerning sexual expression in the digital realm.

Cyber laws in Bangladesh have undergone several changes over the last two decades. The Information and Communication Technology (ICT) Act, 2006, was the first major law governing online communications. However, it became controversial due to Section 57, which employed vague terms such as "offensive" or "defamatory."[10] This provision was often misused to arrest people for their online posts. In 2018, the Digital Security Act (DSA) came into effect, repealing section 57 of the ICT Act, but carried over many of the same issues. Under Sections 25, 29, 31, and 32, the DSA addressed issues like defamation, incitement, and surveillance.[11] Many civil society groups, lawyers, journalists, and human rights activists have criticized it for unclear language and highlighted how it allowed political misuse and restricted free speech, especially for journalists, women's rights activists, and online creators.[12] In 2023, the DSA was replaced by the Cyber Security Act (CSA), but it retained most of its repressive provisions, and still offered very few protections against gender-based violence online[13]. It also failed to clearly define important concepts like affirmative consent or data privacy. As a result, all these laws, ranging from the ICT Act to the CSA, have failed to adequately protect people, particularly women and other marginalized groups, from online abuse.

The Penal Code of 1860, based on colonial ideology, still enables prosecutions for obscenity (Section 292), and crimes against

8 Nari O Shishu Nirjatan Daman Ain, 2000. < http://bdlaws.minlaw.gov.bd/act-835.html>

9 Nari O Shishu Nirjatan Daman (Amendment) Ain, 2020. <http://bdlaws.minlaw.gov.bd/act-details-1351.html>

10 'ICT Act 2006' <https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf>.

11 ডিজিটাল নিরাপত্তা আইন, ২০১৮ (Digital Security Act, 2018)' <http://bdlaws.minlaw.gov.bd/act-1261.html>.

12 Julian Rafah, 'A case against the Digital Security Act 2018' *The Daily Star* (online, 7 April 2023) https://www.thedailystar.net/law-our-rights/news/case-against-the-digital-security-act-2018-3291166; Office of the United Nations High Commissioner for Human Rights (OHCHR), Technical Note on the Review of the Digital Security Act (June 2022) http://ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf.

13 Facts & Norms Institute, *Digital Education and Online Protection of Young People: An Input to the United Nations High Commissioner for Human Rights regarding Bangladesh* (Submission to the Office of the High Commissioner for Human Rights, June 2023) https://www.ohchr.org/sites/default/files/documents/issues/digitalage/cfis/hrc57-promote-digital-education-young-people/subm-solutions-promote-digital-cso-facts-norms-institute.pdf.

women's "modesty" (Sections 354 and 509).[14] These provisions look to patriarchal and moralistic norms, assuming women's virtue. Existing laws are ineffective in addressing issues of queer identity, gender expression, and sexuality in the digital space, and more broadly. Discussions around gender and sexuality are either disregarded or viewed as offensive, particularly when they deviate from heterosexual and binary norms. Therefore, rather than shielding people from harm, the existing legal framework creates the potential to be used to police and punish identity expressions, especially for people with queer and non-heteronormative identities.

This has given rise to a growing need for legal protections that address cyber victimization, including online harms such as NCII, cyberstalking, and digital harassment. Instead of amending existing laws through community-informed, systematic reform, the government chose to pass a new piece of legislation that fails to sufficiently extend the scope of protection to vulnerable communities, especially in light of increasing concern about online abuse.[15]

3. THEORETICAL FRAMEWORK

At the heart of Section 25 is the concept of consent, a legally core but culturally contentious idea. While the provision seeks to criminalize the non-consensual dissemination of intimate content, it does not specify what exactly constitutes consent. It also does not clarify how consent is ascertained, and whose consent matters.

To address these gaps, this paper draws upon feminist legal theory and intersectionality, which provide critical lenses for understanding the construction and regulation of sexual agency, online intimacy, and gendered vulnerability by the law.

Feminist legal theorists have long asserted that the law tends to be insensitive to women's autonomy.[16] It tends to talk about sexuality in terms of harm or morality, as opposed to positive, contextual consent.[17] Catharine MacKinnon critically analyzed how the law breaks sexual violence down into individualized harm, ignoring the broader structures of gender inequality that shape experiences of coercion, silence, and shame.[18] Similarly, Sonia Katyal and other queer legal theorists have underscored how cyber and digital legislation have come to be utilized as heteronormative means of regulation.[19] They are against queer expressions of intimacy, especially in cultures that have already criminalized or marginalized non-normative sexualities.[20]

Drawing upon Kimberle Crenshaw's intersectional perspective, consent cannot be defined outside of the social and legal contexts in which it is assumed to be present or absent.[21] Race, ethnicity, religion, gender, sexuality, optimized digital access, and class intersect in unique ways to influence people's vulnerabilities to experiencing cyberviolence. It can also shape their capacity to report harm and to be able to seek redress.[22] For instance, a rural, adolescent girl accused of "indecency" in

14 'The Penal Code, 1860' <http://bdlaws.minlaw.gov.bd/act-11.html>.
15 'Protecting Women and Children in Cyberspace' (2 January 2025) <https://www.newagebd.net/post/opinion/256835/protecting-women-and-children-in-cyberspace?utm_source=chatgpt.com>.
16 Catharine A MacKinnon, 'TOWARD A FEMINIST THEORY OF THE STATE'.
17 ibid.
18 ibid.
19 Sonia K Katyal, 'The Numerus Clausus of Sex'.
20 ibid.
21 'Mapping-the-Margins.Pdf' <https://supportny.org/wp-content/uploads/2018/04/mapping-the-margins.pdf>.
22 ibid.

a social media video not only faces further harassment and discrimination through abuse of the legal system, and impaired access to justice and remedies, she also has to contend with family violence, possible expulsion from school, and social isolation. All of these factors, and more, complicate the narrative of consent as a simple 'yes' or 'no'.

In the digital context, 'criminalizing revenge porn' highlights that the legal framework needs to account for new modes of intimacy, power, and surveillance enabled by technology.[23] Unlike traditional crimes, harms such as non-consensual image sharing impact on victims' experiences of safety and dignity in the digital space.[24] However, as Radhika Gajjala and Nanjala Nyabola have argued, legal processes in postcolonial contexts frequently ignore the digital agency of vulnerable and marginalized users.[25]

Consequently, this paper seeks to apply a theoretical approach that understands consent not just as a legal concept but as a relational and political construct situated within structures of power. This study argues that section 25 can be an effective safeguard if it explores a visionary, transformative notion of legal consent.

4. CRITICAL ANALYSIS OF SECTION 25

Section 25 of the Cyber Protection Ordinance, 2025, is the first in Bangladeshi history to legally criminalize the sharing of, or threats to share, intimate content non-consensually. It is a clear reaction to a growing crisis of digital harm, particularly those relating to NCII. It is also known as "revenge porn," as well as other image-based sexual exploitation.[26]

NCII has replaced the outdated expression "revenge porn," which is noteworthy.[27] In most cases, revenge entails hurting someone in retaliation for perceived wrongdoing.[28] However, offenders may act out of malice, or out of a desire for money, fame, or amusement, rather than simply because of a desire for revenge. Further, the use of the term "pornography" runs the risk of centering victim-blaming narratives, through implying that complainants and/or survivors of NCII are willing participants or somehow complicit in the non-consensual distribution of their intimate images. Additionally, it portrays a harmful act as a form of entertainment.[29] However, the Cyber Protection Ordinance continues to use this outdated terminology, when it was crucial for the new framework to change it and match and reflect complainants' and survivors' experiences, rather than promoting moralistic or simplistic views of harm.

Considering the definitions provided in Section 2 for 'digital child sexual abuse material', 'sexual abuse', 'revenge porn', and 'sextortion', all these offenses fall within the purview of Section 25 of the Cyber Protection Ordinance, which details offences related to sexual harassment, blackmail, and the

23 Danielle K Citron and Mary Anne Franks, 'Criminalizing Revenge Porn'.

24 ibid.

25 Radhika Gajjala, *Cyberculture and the Subaltern* (Lexington Books, 1st ed, 2012) < https://www.bloomsbury.com/us/cyberculture-and-the-subaltern-9780739118542/>; Nanjala Nyabola, *Digital Democracy, Analogue Politics: How the Internet Era Is Transforming Politics in Kenya* (Zed Books, 1st ed, 2018).

26 'সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫ (Cyber Protection Ordinance, 2025)' (n 5).

27 'Non-Consensual Sharing of Intimate Images', *eReader* <https://www.mediadefence.org/ereader/publications/online-violence-against-journalists/module-2-digital-attacks-and-online-gbv/ncii/>.

28 'Revenge Definition & Meaning | Britannica Dictionary' <https://www.britannica.com/dictionary/revenge>.

29 Non-Consensual Sharing of Intimate Images (n 28). .

publication of obscene consent, via digital or electronic means, and the corresponding penalties for these offences.[30] According to the provision, if the victim is either a woman or a child, the offence carries the penalty of up to five years' imprisonment or BDT 20 lakh in fine. In case of a male victim above the age of 18 and, presumably applicable to all other victims irrespective of gender, the maximum penalty is two years' imprisonment or BDT 10 lakh.[31] While this difference in sentencing is presented as a gender-sensitive approach to the recognition of structural violence against women and the disproportionate impact of such violence on women and children, this author argues that the provision reflects patriarchal assumptions regarding vulnerability, agency, and victimhood in the virtual space.

In this context, feminist legal theories addressing the concepts of 'victim feminism' and 'agency feminism' are particularly relevant. Agency feminism is a more recent development in feminist legal theories than victim feminism. Victim feminism developed during the 1960s through the then prominent feminist writers like Betty Friedan[32] and Germanine Greer.[33] Criticism against it started to emerge after the 1990s through writers including Katie Roiphe[34] and Naomi Wolf.[35] Victim feminism essentially identifies women with a particular kind of victim subject: a passive, helpless, innocent victim subject who lacks strength, self-knowledge and the capacities for self-reliance and personal responsibility.[36] Against this view, Roiphe and Wolf argue in their works, that emphasis on victimization reinforces the sex-stereotypical views of women, and suggest that the emphasis should instead be on women's individual agency, choice, and exercise of responsibility.[37] The difference in sentencing as prescribed in Section 25(3) is a vivid example where women's victimhood is prioritized over their agency, reinforcing the stereotypical view of women.

The language of Section 25 is notable for its lack of legal precision. Terms like "intimate content" and "consent," are left undefined in the ordinance. This kind of ambiguity invites irrational judgment by the law and judiciary. In a culture of moral surveillance, shaped legal order can lead to the criminalization of consensual sexual expression. Rather than operating as a shield for digital autonomy, the provision risks functioning as a tool for regulating morality, often under pressure from social, familial, or religious norms in Bangladesh.

Beyond its legal ambiguities, Section 25 must also be understood through a criminalization lens. While Article 27 of the Constitution of Bangladesh guarantees equality before the law, Article 28(4) additionally allows the State to make special provisions for women, children, or any "backward section of citizens."[38] The ostensibly gender-sensitive sentencing for women and child victims under Section 25 is aligned with this constitutional

30 ibid.
31 ibid.
32 Betty Friedan, *The Feminine Mystique* (Penguin Books, London 1963).
33 Germanine Greer, *The female eunuch* (Paladin, London 1971).
34 Katie Roiphe, *The Morning After: Sex, Fear and Feminism* (Hamish Hamilton, London 1993).
35 Naomi Wolf, *Fire with Fire: The New Female Power and How It Will Change the Twenty-First Century* (Chatto & Windus, London 1993).
36 Rebecca Stringer, *Knowing Victims: Feminism, Agency and Victim Politics in Neoliberal Times* (1st edn, Routledge 2014) 27.
37 Roiphe (n 34) 29-50; Wolf (n 35) 149, 185.
38 'The Constitution of the People's Republic of Bangladesh' <http://bdlaws.minlaw.gov.bd/act-367.html>.

dictate. However, the provision fails to extend the scope of this gender-sensitive approach, and its overall protection, to members of the Hijra community, who are officially recognized as the 'Hijra gender' by virtue of a gazette published by the Ministry of Social Welfare in 2014,[39] following a Cabinet decision in 2013 to recognize Hijras as a separate gender and to reflect their presence in national identification documents and censuses,[40] which was a move to acknowledge the marginalized, at-risk status of the Hijra community and integrate them into government social welfare schemes. Notably, this recognition, and any ensuing social protections, apply only to Hijra community members, not transgender individuals or people with other non-normative gender identities who do not identity as Hijra.

While there is significant debate about the two feminist theories regarding women's victimhood and their agency, the Hijra community's status of victimhood, especially in the context of Bangladesh is unambiguous. Hijra community members face high levels of online harassment, extortion, and sexual abuse.[41] Despite the recognition and the state's tacit acknowledgment of the vulnerabilities faced by Hijras, the Cyber Protection Ordinance does not provide any special protection for them against their increased vulnerability online, even though gender non-conforming individuals, including Hijra community members and transgender individuals, encounter various barriers to justice and lack access to basic services. These barriers include police insensitivity, service providers who are not gender responsive, societal stigma, and a lack of gender-affirming legal processes, which make them even more vulnerable to cyber violence. While Article 28 of the Constitution does not explicitly define "any backward section of citizens", the guarantees of this constitutional provision are understood to extend to vulnerable individuals and communities at risk, facing social equalities and varying degrees of discrimination and marginalization. All individuals embodying gender and sexual identities beyond heteronormative binaries, including Hijra community members and transgender individuals, fall within its ambit. Had the Ordinance provided safeguards that addressed the specific vulnerabilities of such groups, communities, and bodies, it would have reflected the spirit of both Articles 27 and 28, thereby upholding commitments to protect those at greatest risk, from discrimination at the hands of the justice system.

In Bangladesh, like in much of South Asia, young people, particularly with low socio-economic status, rural populations, unmarried people, especially women, and religious minorities, are much more likely to face criminalization. They are often accused of vague concepts like "obscenity" or "indecency" in society. Unfortunately, existing laws provide no precise legal definition for such terms. Here, legal protections are not indifferent. They work through unequal systems of power and strong, patriarchal understandings of morality.

The lack of procedural safeguards also compounds the risk of abuse. The Ordinance does not require judicial authorization before investigation or arrest. It also does not provide clear standards for evidence collection, cyber

39 Government of the People's Republic of Bangladesh, Ministry of Social Welfare (2014), Bangladesh Gazette, Circular No. MoSW/'Kormo'/'Sha'/Hijra-15/2013-40. <https://www.dpp.gov.bd/upload_file/gazettes/6851_39605.pdf>

40 Bdnews24 (2013), 'Third gender' gets state recognition, 11 November 2013. < https://bdnews24.com/bangladesh/third-gender-gets-state-recognition>

41 Ayesha Siddequa Daize and Essaba Masnun, 'Exploring the Socio-Economic and Cultural Status of Third Gender Community in Bangladesh'.

forensics, and protection of confidentiality and anonymity for complainants and survivors. This opens up possibilities for baseless claims, politically motivated prosecution, and morality policing. In this case, the most vulnerable people are public figures, content creators, and activists who use the internet. There is no mention of a victim-survivor protection framework for psychological services and safe channel reporting. This fails to provide the proper protection to the individuals.

There is a lack of coordination between Section 25 of the Cyber Protection Ordinance 2025 and other relevant laws, such as the Pornography Control Act 2012 and the Cyber Security Act 2023. Lack of harmonization results in inconsistent enforcement, overlapping jurisdictions, and procedural ambiguity. It can cause contradictory court rulings and obstacles to justice for both defendants and complainants. The ordinance's efficacy is diminished by this fragmentation, which also runs the risk of eroding public trust in its authority and capacity to provide just, open, and consistent results.

5. RELATED EXISTING LAWS IN SOUTH AND SOUTHEAST ASIA

The issues in Section 25 of Bangladesh's Cyber Protection Ordinance 2025 are not new. There are already existing laws in South and Southeast Asian countries, responses to online gender-based violence, digital consent, and intimate content regulation.[42] The continuing tension between rights-based protections and patriarchal control strongly reflects the regional politics of cyber law through these existing laws.

In India, laws such as the Information Technology Act (2000), particularly Section 66E and Section 67, criminalize online transmission of "obscene" or "sexually explicit" matter.[43] The terms are, however, not defined. They are also culturally loaded and therefore subject to subjective interpretation. For instance, the consensual sharing of intimate content among teens has sometimes been dealt with as criminal under IT law as well as under the Protection of Children from Sexual Offences (POCSO) Act (2012).[44]

Similar regulations to Section 25 are found in Pakistan's Prevention of Electronic Crimes Act (PECA) 2016, specifically Section 21 on the "unauthorized use of identity information" and "modesty."[45] From the socio-cultural context of Pakistan, when a female victim is involved, the severity of the punishment is increased. However, the rule is frequently utilized to punish rather than to safeguard female visibility online, namely targeting journalists, LGBTQ people, and female social media users. Digital consent is also marginalized here in favor of upholding ideas of "honor" and "dignity," which serves to further a legal culture that is based on surveillance.

Indonesia's Law No. 12 of 2022 on Sexual Violence Crimes is noteworthy because it explicitly recognizes online gender-based violence, such as non-consensual dissemination of intimate images, digital coercion, and cyber harassment.[46] This is a step forward. Yet,

42 'Digital-Governance-and-Rights-in-South-Asia-and-the-Path-Forward.Pdf' (n 2).

43 'Information Technology Act, 2000' <http://indiacode.nic.in/handle/123456789/1999>.

44 'THE PROTECTION OF CHILDREN FROM SEXUAL OFFENCES ACT, 2012' <https://www.indiacode.nic.in/bitstream/123456789/2079/1/AA2012-32.pdf>.

45 'Prevention of Electronic Crimes Act, 2016' <https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjjj>.

46 'LAW OF THE REPUBLIC OF INDONESIA, NUMBER 12 OF 2022' <https://lpr.adb.org/sites/default/files/resource/%5Bnid%5D/indonesia-anti-sexual-violence-law-uu-tpks-nomor-12-tahun-2022-tindak-pidana-kekerasan-seksual-english.pdf>.

implementation remains inconsistent. As noted, concerning Bangladesh's Section 25, Indonesia's law is also unclear regarding procedure, relying heavily on law enforcement discretion.

In the context of Nepal, the Electronic Transactions Act (2008) criminalizes the publishing or transmission of "improper" content, which includes materials defined as against "public decency."[47] There is no specific acknowledgment of digital consent or NCII, which contributes to large-scale underreporting and victim shaming. Researchers from LOOM and the EROTICS South Asia network have identified how ambiguous legal language and patriarchal enforcement practices thus shift the shame onto victims instead of the perpetrators.[48]

Nepal's Criminal Code includes several rules that aim to regulate morality and public order. However, these rules pose significant threats to freedom of expression and privacy, particularly for marginalized communities. Section 121 makes "obscene" content illegal without considering consent. This may lead to the criminalization of consensual sexual expression. Sections 293 and 294 recognize consent in recording and sharing information but can restrict press freedom and public discussion. Section 306 deals with defamation, while Section 122 addresses "obscene" behavior. Both use vague terms like "vulgar" or "immoral," which can suppress legitimate sexual expression and promote moral policing. These laws enable surveillance and disproportionately impact groups such as sex workers, trans individuals, and young women.[49]

Sri Lanka does not have any specific provisions on cyber violence. Though they have the Computer Crimes Act (2007), which prioritizes breaches of a computer system and hacking, there is no rights-based understanding of digital consent and protection against NCII.[50] Moreover, the country continues to criminalize same-sex relationships under its colonial sodomy laws (Sections 365 and 365A), which adds risk for queer individuals facing cyber-harassment.[51]

Considering the laws, they show a regional legal pattern by recognizing the potential of cyber violence. There is a common phenomenon of having vague terminology and controlling the law from a patriarchal system. Overall, these laws often fail to account for intersectional vulnerabilities, particularly of those outside normative gender and sexual categories.

6. CONCLUSION

Section 25 of the Cyber Protection Ordinance 2025 represents a remarkable shift in the evolution of Bangladeshi cyber law. It offers long-awaited legal recognition of the harms of non-consensual intimate images and digital sexual violence. But, as illustrated in this article, the provision is undermined by structural limitations. Section 25's unequal punishments, vague language, and weak safeguards reflect a broader South Asian pattern. Those who treat digital harm as sexual misconduct focus more on moral control than

47 'The Electronic Transactions Act, 2063 (2008)'.
48 'EROTICS South Asia Exploratory Research: Sex, Rights and the Internet' (n 7).
49 Body & Data. ('year'), 'Mapping Laws Relevant to Online Violence in Nepal: A Study'. LINK
50 'Computer Crime Act' <https://www.srilankalaw.lk/revised-statutes/alphabetical-list-of-statutes/239-computer-crime-act.html>.
51 'Penal Code Ordinance No 2 of 1883 (Sri Lanka)' <https://citizenslanka.org/wp-content/uploads/2016/02/Penal-Code-No-02-of-1883-E.pdf>.

on digital rights. By prioritizing women and children, the law overlooks queer, trans, and male victims, leaving their abuse invisible and ignored.

There arises a big concern regarding the issue of consent. Instead of protecting autonomy, it may be used to control sexuality. Especially non-traditional expressions due to the socio-cultural barriers.

Bangladesh must reform Section 25 as part of a broader vision of inclusive digital justice. This includes not only reforming the law but also reforming institutions to ensure inclusivity. The law should include equal protection, consent-based explicit rules, fair procedures, and adequate survivor support. The law has to accommodate that all have the right to express intimacy and pursue justice regardless of gender, sexuality, or class. With these changes, Section 25 can become a powerful instrument for dignity, autonomy, and equality within the digital realm.

About the Authors

Nabangsu Chakma is a law graduate from the University of Dhaka, Bangladesh. He is currently a Legal Consultant to the UN Special Rapporteur on the Rights of Indigenous Peoples. His interests lie at the intersection of law, human rights and technology.

Nazifa Muniyat Quader, Lecturer of Canadian University of Bangladesh and a Legal Advisor to a climate-tech startup, is an accomplished Academic and legal professional with experiences in legal practice and development sector. She previously worked at the United Nations Office of Drugs and Crime (UNODC) as a team member on the GLO.ACT project. Additionally, she serves as an adjudicator in National and International Moot Court Competitions. Her research interests lie in – international diplomacy, intellectual property, humanitarian law, refugee law, and personal laws.

Afrida Samiha Nabilah is a researcher specializing in human rights, gender justice, and social inclusion. As a Research Assistant at BLAST, Afrida has worked on Bangladesh's Disability Rights and Protection Act and advocated for the rights of religious minorities and gender-diverse groups. She was awarded the Community Equity Fellowship by BLAST, where she conducted in-depth research on the employment rights of plainland indigenous women. Afrida is an active member of the Cyber Support for Women and Children (CSWC), addressing digital rights issues and providing legal aid to victims of violence. Her research interests include the rights of marginalized communities, technology-facilitated gender-based violence, migration, and refugee issues.

Saraban Tahura Zaman, a human rights lawyer, consultant, and feminist activist from Bangladesh, works as a Consultant for Global Advocacy at the Center for Reproductive Rights. A diploma holder in Leadership from the Swedish Institute in 2018, she led the SheDecides movement in Bangladesh and curated a global exhibition

commemorating the 25th anniversary of the Beijing Declaration. She was also a core member of the Drafting Committee for the Transgender Protection Bill. As a policy analyst, she has contributed to the review of key laws and policies, including the Child Marriage Restraint Act, Anti-Discrimination Law, and ICT Act. Additionally, Ms. Zaman is the founder of Justicia Feminist Network, the first legal network of feminist lawyers in Bangladesh, dedicated to advancing a more gender-just society.

Tabassum Nuha, Lecturer in the Department of Mass Communication and Journalism at Bangladesh University of Professionals (BUP), is affiliated with the Society for Environment and Human Development (SEHD) and the Bratyajan Research Center (BRC). She previously served as a researcher at the Liberation War Museum. Her academic research interests include digital media communication, information disorder, and cultural studies.

digitally right

www.digitallyright.org

© 2025 Digitally Right Limited. All rights reserved.