A NEW DIGITAL FRONTIER

A Roadmap for Rights-Respecting Digital Governance Laws in Bangladesh

Second Edition

Shahzeb Mahmood

WHITE PAPER

A NEW DIGITAL FRONTIER

A Roadmap for Rights-Respecting Digital Governance Laws in Bangladesh

Second Edition

Shahzeb Mahmood

Copyediting by ***Nicole Lim***

Publication design by ***Monirul Islam***

ACKNOWLEDGEMENT

This white paper was prepared through extensive research, consultation, and engagement with a wide range of stakeholders working across human rights, civil society, academia, governance, law, industry, and the broader digital and technology policy ecosystem. The author is grateful to those who generously shared their expertise, experiences, and perspectives throughout the development of this paper. Specifically, the author acknowledges the valuable comments, feedback, and insights provided by external researchers, practitioners, policymakers, and subject-matter experts who participated in consultations and informal discussions during the research and review process. Special appreciation is extended to colleagues at Tech Global Institute, especially Shahnewaj Patwari and Fowzia Afroz, whose research, administrative, logistical, and editorial support contributed to the completion of this project. Any errors, omissions, or views expressed in this publication remain solely those of the author and do not necessarily reflect the views of the individuals or organizations who contributed to the research, consultation, or review process.

TABLE OF CONTENT

ABBREVIATIONS

AI	means artificial intelligence.
Bangladesh Police	means the police force established under the *Police Act, 1861* (Act No. V of 1861) and other applicable laws of Bangladesh, and includes different specialized units and departments.
BDT	means Bangladesh Taka, the lawful currency of Bangladesh.
BFIU	means the Bangladesh Financial Intelligence Unit established under the *Money Laundering Prevention Act, 2012* (Act No. V of 2012).
BTRC	means the Bangladesh Telecommunication Regulatory Commission established under the *Bangladesh Telecommunication Act, 2001* (Act No. XVIII of 2001).
Competition Commission	means the Bangladesh Competition Commission established under the *Competition Act, 2012* (Act No. XXIII of 2012).
CSAM	means child sexual abuse material; that is, any material, content, or representation, including images, videos, audio recordings, text, or digital media, that depicts, describes, promotes, facilitates, or involves the sexual exploitation, abuse, grooming, or sexually explicit depiction of a child, whether real or simulated.
Constitution	means the *Constitution of the People's Republic of Bangladesh*.
DGFI	means the Directorate General of Forces Intelligence, the defense intelligence agency of Bangladesh, operating under the Bangladesh Armed Forces.
DNCRP	means the Directorate of National Consumers' Right Protection established under the *Consumers' Right Protection Act, 2009* (Act No. XVI of 2009), and, accordingly, DG-DNCRP should be construed as Director General of the Directorate of National Consumers' Right Protection.
EU	means the European Union.
FAANG+	refers to large multinational technology and digital platform companies, including companies such as Meta (Facebook), Amazon, Apple, Netflix, Alphabet (Google), Microsoft, ByteDance (TikTok), X (formerly Twitter), OpenAI (ChatGPT), Tencent, Alibaba, and other similar technology firms.
GDPR	means the *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, and repealing Directive 95/46/EC (General Data Protection Regulation)*.
ICCPR	means the *International Covenant on Civil and Political Rights* adopted by the United Nations General Assembly in 1966, and acceded to or ratified by the government of Bangladesh in 2000.

Intelligence Agencies	means government organizations tasked with gathering, analyzing, and managing information related to national security, foreign intelligence, and internal threats, and engaging in surveillance, espionage, and counterintelligence; it includes, without limitation, BFIU, BTRC, DGFI, NCPA, NSI, NTMC, and specialized units and departments within Bangladesh Police, such as the Special Branch, Detective Branch, Criminal Investigation Department, Rapid Action Battalion, and Counter Terrorism and Transnational Crimes unit.
LEA	means law enforcement agencies, including Bangladesh Police, as well as the Intelligence Agencies.
NCPC	means the National Cyber Protection Council established under the *Cyber Protection Act, 2026* (Act No. LXXXI of 2026).
NCPA	means the National Cyber Protection Agency established under the *Cyber Protection Act, 2026* (Act No. LXXXI of 2026), and, accordingly, *DG-NCPA* should be construed as Director General of the National Cyber Protection Agency.
NDMA	means the National Data Management Authority established under the *National Data Management Act, 2026* (Act LXXX of 2026).
NDMPB	means the National Data Management Policy Board established under the *National Data Management Act, 2026* (Act LXXX of 2026).
NRDEX	means National Responsible Data Exchange established under the *National Data Management Act, 2026* (Act LXXX of 2026).
NSI	means the National Security Intelligence, the civilian intelligence agency of Bangladesh, operating under the Prime Minister's Office.
NTMC	means the National Telecommunication Monitoring Centre, the national intelligence, surveillance and interception agency of Bangladesh, operating under the Ministry of Home Affairs.
TFSV	means technology-facilitated sexual violence; that is, any content, including still images, videos, audio recordings, and digital media, that visually or audibly depicts sexual violence, coercion, or exploitation, including non-consensual or digitally manipulated pornography, sextortion, cyberstalking, online sexual harassment, and the dissemination of explicit content without consent, that is enabled, amplified, or carried out using digital technology.

SCOPE OF THE PAPER

This white paper provides a focused and actionable analysis of critical aspects of the regulatory framework for the digital ecosystem in Bangladesh, with particular emphasis on online safety and content regulation, cybersecurity, privacy and data protection, surveillance, competition, and consumer protection in the digital domain. Our focus extends to substantive issues such as definitions, extraterritorial application of laws, and the scope of regulatory authority, alongside systemic reforms including sentencing guidelines, the development of a centralized case-tracking system, and differentiated legal treatment to appropriately address varying degrees of offenses. We further provide analyses from comparable legislations and policies in different countries.

While the white paper prioritizes substantive and structural issues due to their urgent attention, certain areas relevant to the digital ecosystem fall outside its immediate scope, including intellectual property rights, mobile and digital financial services, foreign exchange regulations, digital signature certification, and critical information infrastructure protections. Future efforts may revisit these excluded areas, however, this white paper is intentionally focused on addressing some of the most pressing issues that demand urgent intervention during the present period of democratic transition. The overarching goal is to provide a blueprint for the formulation of a robust, balanced, and rights-respecting regulatory framework that protects digital rights, foster innovation, and ensure a competitive and consumer-friendly digital environment.

The white paper is structured into two parts, each addressing distinct aspects of legal and regulatory reforms, including analyses of specific provisions needed to strengthen Bangladesh's information and technology governance framework.

Part A focuses on essential revisions across eight key legislations that underpin the existing regulatory environment: the *Personal Data Protection Act, 2026*, the *National Data Management Act, 2026*, the *Cyber Protection Act, 2026*, the *Bangladesh Telecommunication Act, 2001,* the *Penal Code, 1860*, the *Pornography Control Act, 2012*, the *Competition Act, 2012*, and the *Consumer Rights Protection Act, 2009*. These revisions aim to modernize outdated provisions, address definitional ambiguities, and enhance their effectiveness in the digital age.

Part B outlines essential enactments required to address gaps in the legal landscape, proposing four new legal frameworks: the *Online Safety Act*, the *Regulation of Investigatory Powers Act*, the *Digital Commerce Act*, and a forward-looking Artificial Intelligence Strategy. Collectively, these provide a comprehensive roadmap for reform, ensuring a robust, equitable, rights-respecting legal regime.

We provide a comprehensive, albeit non-exhaustive, list of laws applicable to technologies and are salient to fundamental rights online. However, we prioritize key statutes that we assess as critical and urgent in the reform process to ensure Bangladesh takes a first step towards inclusive, rights-respecting digital governance.

GUIDING PRINCIPLES AND CONSIDERATIONS

While drafting the white paper, we used the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights*, and the *United Nations Guiding Principles on Business and Human Rights* as key benchmarks, alongside comparative legislations, regulatory frameworks, jurisprudence, and policy instruments from other jurisdictions, with two important caveats.

Firstly, international human rights laws are not without criticism — often debated as "Eurocentric" because of their historical development and, at times, selective or politicized application by powerful states — and subject to uneven implementation and enforcement across jurisdictions, particularly amid shifting geopolitical dynamics since the early 2020s. Nevertheless, they provide an important normative foundation and enjoy broad support from governments, civil society, academia, and technical communities, and have served as widely recognized frameworks for governance norms for over 70 years.

Secondly, while comparative legislations and foreign regulatory frameworks have been referenced to support proposed reforms in Bangladesh, this paper does not necessarily endorse those frameworks or the broader policy environments in which they operate; rather, they are used selectively as comparative reference points for identifying regulatory approaches, safeguards, institutional mechanisms, and governance models relevant to the Bangladeshi context.

It is also worth noting that "technolegalism" — the use of technology-driven or algorithmic systems to interpret, train, and comply with legal and regulatory frameworks, or a compliance-first approach to digital governance — should be approached with caution. While legislations and policies offer important mechanisms to mitigate specific types of harms, they are not a universal solution for addressing the complexities of diverse human conditions, ethical dilemmas, and social and political realities; human discretion, contextualization, and democratic accountability remain essential to ensure digital technologies serve the public interest and safeguard fundamental rights.

Moreover, we emphasize that legal reforms alone cannot resolve deep-rooted sociopolitical and economic inequalities and inequities that influence how technologies are designed, deployed, commercialized, and regulated. Although this paper focuses on structural legal issues, we urge readers, policymakers, and relevant stakeholders to complement legal developments with nuanced societal, institutional, educational, economic, and political interventions.

The legal frameworks analyzed in this paper primarily focus on Bangladesh. However, similar patterns of colonial-era statutes, executive overreach, legal fragmentation, weak institutional safeguards, and repressive practices are evident in many parts of the world. We hope this paper serves as a starting point for analysis and reform of comparable legal frameworks elsewhere, and is particularly relevant and actionable in resource constrained political environments within the Global South.

EXECUTIVE SUMMARY

Bangladesh's rapid digitization has accelerated economic growth, expanded connectivity, and transformed social, political, and commercial life. However, these developments have also exposed significant regulatory and institutional weaknesses, as the state has sought to govern an increasingly digital society through legal frameworks that remain fragmented, inconsistently enforced, and insufficiently adapted to the realities of a digital-first ecosystem. Since publication of the first edition of this white paper in 2024, successive administrations have introduced multiple legislative reforms and ordinances — most recently in April 2026 — aimed at restructuring Bangladesh's digital governance framework. Nevertheless, these reforms have largely failed to resolve underlying structural concerns relating to constitutional compliance, legal certainty, institutional independence, procedural safeguards, and alignment with international human rights standards.

The primary legislative instruments governing digital activities — including the *Cyber Protection Act, 2026*, the *Personal Data Protection Act, 2026*, the *National Data Management Act, 2026,* the *Bangladesh Telecommunication Act, 2001*, the *Information and Communication Technology Act, 2006*, and other laws — present a paradox. While these laws purport to secure cyberspace, regulate digital services, and protect public interests, they frequently do so through overbroad powers, vague definitions, weak safeguards, and disproportionate enforcement mechanisms that risk undermining constitutional rights, democratic accountability, innovation, and economic growth. Additionally, despite their protective intent, laws such as the *Children Act, 2013*, the *Prevention of Women and Children Repression Act, 2000*, and the *Pornography Control Act, 2012* remain ill-equipped to effectively address evolving forms of online harms, including child sexual abuse material, technology-facilitated sexual violence, deepfake abuse, coordinated online harassment, and other digitally mediated harms, particularly against women, children, minorities, and other vulnerable or marginalized communities. Similarly, legislative frameworks such as the *Competition Act, 2012* and the *Consumers' Right Protection Act, 2009* were designed primarily around traditional markets and consumer relationships, rendering them insufficiently equipped to address the complexities of digital platform economies, algorithmic market power, data-driven business models, and emerging forms of digital consumer harm.

These legislative developments must also be understood within Bangladesh's complex socioeconomic and political realities. A substantial number of digital and security-related laws were enacted or amended during the 16-year administration under former Prime Minister Sheikh Hasina Wazed, during which institutions — including the security sector, media, and judiciary — became increasingly centralized and executive-driven. As a result, many of these frameworks failed to adequately address structural inequalities and vulnerabilities affecting women, children, minority communities, political dissidents, journalists, and civil society actors, both offline and online. Over the subsequent transitional period, the interim administration enacted an unprecedented number of ordinances (over 130, including several significantly affecting digital governance) often within compressed timelines and with limited public consultation or institutional deliberation. While some reforms reflected attempts to modernize the legal framework, many continued to raise concerns regarding legislative quality, institutional readiness, constitutional safeguards, and consistency with domestic and international human rights standards. Following the subsequent formation of government by the Bangladesh Nationalist Party in early 2026, several of these ordinances were retained or enacted with only limited substantive revision, underscoring the continuing need for a more consultative, transparent, and rights-respecting lawmaking process.

Of particular concern is the manner in which constitutional structures and institutional arrangements have evolved in practice. Bangladesh's Constitution — despite drawing inspiration from instruments such as the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political*

Rights — has frequently been interpreted and operationalized in ways that facilitate concentration of executive authority while weakening parliamentary accountability and judicial independence. Particularly, the Westminster-style parliamentary system, intended to ensure democratic oversight through a cabinet accountable to parliament, has increasingly enabled executive dominance over state institutions, and often marginalizing opposition voices and limiting institutional checks and balances. Compounding these issues, the judiciary, which could have served as a bulwark against these trends, has often failed to rise to the challenge; rather than championing a forward-leaning, rights-respecting approach, judicial approach toward digital governance and speech-related restrictions have often adopted broad and deferential interpretations of "reasonable restrictions," particularly in relation to speech, privacy, public order, and national security. The absence of narrowly tailored standards, robust proportionality analysis, and sufficiently reasoned jurisprudence has contributed to legal ambiguity and increased scope for arbitrary enforcement, undermining the Constitution's role as a safeguard for democratic governance and fundamental rights.

One of the core structural issues across Bangladesh's digital governance framework is the overbroad and ambiguous nature of many regulatory provisions, including poorly constructed definitions and expansive discretionary powers conferred upon policymakers, regulators, and law enforcement agencies. For instance, despite recent amendments, the *Bangladesh Telecommunication Act, 2001* continues to authorize extensive surveillance, interception, and information-control powers with limited independent oversight or meaningful procedural safeguards. Similarly, the *Cyber Protection Act, 2026* criminalizes categories of online conduct through vague and insufficiently defined terminology, including concepts such as "disorder" or threats to "communal harmony," creating significant risks of subjective interpretation, overbroad enforcement, and encroachment upon lawful expression. Likewise, key terms such as "pornography" under the *Pornography Control Act, 2012* remain excessively broad, outdated, and technologically inadequate. Collectively, these frameworks have historically contributed to criminalization of online dissent, self-censorship, selective enforcement, suppression of opposition voices, and erosion of public trust in state institutions.

The broader regulatory architecture governing Bangladesh's digital ecosystem also reflects a predominantly security-centric approach. Key regulatory and enforcement institutions — including the National Cyber Protection Agency, the Bangladesh Telecommunication Regulatory Commission, and various intelligence and surveillance bodies — operate with limited structural independence, weak transparency obligations, and inadequate democratic oversight. More concerningly, intelligence and monitoring entities such as the Directorate General of Forces Intelligence, National Security Intelligence, and National Telecommunication Monitoring Centre continue to operate without sufficiently transparent public mandates, clearly defined oversight structures, or comprehensive procedural safeguards governing surveillance and interception activities. This security-first model is further reinforced by the broad exemptions afforded to law enforcement, intelligence, national security, and public authorities under the *Personal Data Protection Act, 2026*, which may enable existing surveillance, interception, intelligence-gathering, and data-sharing practices to continue with limited meaningful accountability or independent oversight despite the enactment of a comprehensive data protection framework. This concentration of authority within security-oriented institutions has resulted in a governance framework that prioritizes control, surveillance, and content regulation over innovation, accountability, procedural fairness, and protection of individual rights. Such an approach, in its current form, is misaligned both with domestic constitutional obligations and Bangladesh's commitments under the international human rights instruments.

The colonial and postcolonial foundations of many of these frameworks further exacerbate both enforcement and legitimacy concerns. Several contemporary digital laws borrow substantive language, structures, and enforcement philosophies from colonial-era statutes such as the *Penal Code, 1860* and the *Code of Criminal Procedure, 1898*, preserving punitive and executive-centric approaches ill-suited for regulating modern

digital ecosystems. For example, speech-related offenses continue to be heavily criminalized, often coupled with cognizable and non-bailable provisions that enable arrests without warrants, which create strong incentives for self-censorship, particularly among journalists, activists, researchers, academics, and political opponents. At the same time, similar to its predecessor, the *Cyber Protection Act, 2026* continues to consolidate wide governmental authority over online expression, cybersecurity, platform governance, and data-related conduct without adequately distinguishing between fundamentally different categories of offenses or incorporating sufficiently robust safeguards relating to necessity, proportionality, judicial authorization, and due process. This not only risks undermining constitutional protections relating to speech, privacy, association, and access to information, but also creates regulatory uncertainty that may discourage innovation, investment, entrepreneurship, and growth within Bangladesh's emerging digital economy.

Meanwhile, recent legislative efforts also reveal the limitations of extensive legal transplantation without sufficient adaptation to local institutional realities. For example, the *Personal Data Protection Act, 2026* draw heavily from comparative frameworks such as the EU *General Data Protection Regulation*; however, the relative success of the European framework depends upon decades of institutional development, judicial interpretation, regulatory guidance, coordinated enforcement structures, compliance ecosystems, and technical capacity that are not yet fully present in Bangladesh. Although operationalization of certain provisions has been deferred to facilitate compliance preparation, limited institutional readiness, regulatory guidance, technical capacity, and compliance support mechanisms continue to create significant implementation challenges for both public and private actors.

The inadequacy of Bangladesh's digital governance framework extends beyond speech, privacy, and cybersecurity to areas foundational to the functioning of the digital economy itself. While jurisdictions across Europe, South and Southeast Asia, Australia, and the United States have increasingly utilized competition, consumer protection, and platform governance frameworks to regulate dominant technology companies and digital marketplaces, Bangladesh's *Competition Act, 2012* and *Consumers' Right Protection Act, 2009* remains underutilized and poorly calibrated for digital market realities.

Bangladesh therefore stands at a critical juncture in shaping a digital governance framework capable of balancing security, innovation, democratic accountability, economic growth, and protection of fundamental rights. The need for comprehensive, coherent, and rights-respecting reform is increasingly urgent. By adopting the reforms proposed throughout this white paper, Bangladesh has the opportunity to develop a governance model that better aligns with constitutional principles, international human rights standards, technological realities, and the needs of an evolving digital society.

However, legal reform alone will not be sufficient to create an inclusive, equitable, and rights-respecting digital ecosystem. Deep-rooted societal inequalities relating to religion, ethnicity, gender, education, economic disparity, and political polarization continue to shape how technologies are designed, deployed, commercialized, and experienced. Sustainable reform therefore requires not only modernization of legal frameworks, but also broader investments in institutional capacity, digital literacy, independent media, civic participation, technical expertise, competitive markets, and democratic accountability. In absence of a nuanced and comprehensive interrogation and overhaul of digital governance within the constraints of societal structures, even the most well-crafted laws will struggle to address the multifaceted challenges of digital harms and cybersecurity. Effective digital governance must, therefore, remain adaptive, context-sensitive, rights-respecting, technologically neutral, and capable of integrating legal, technical, institutional, and societal dimensions in a manner that both protects rights and enables innovation within an increasingly interconnected digital future. For Bangladesh, this means not only reforming outdated and repressive laws, but also creating an enabling social and political environment that can chart a path toward a more equitable, inclusive and safe digital future, and setting a precedent for other countries grappling with similar challenges.

HEAT MAP OF POTENTIAL HUMAN RIGHTS IMPACT OF THE LEGISLATIONS

We also assessed the potential impact of the selected legislations on fundamental rights in the digital ecosystem and classified them into four categories based on the level of risk.

	HIGH RISK OF ADVERSE IMPACT
	MEDIUM RISK OF ADVERSE IMPACT
	NO RISK OF ADVERSE IMPACT
	POSITIVE IMPACT

For the purposes of this white paper, the human rights implications of six legislations have been examined in relation to three fundamental rights: freedom of expression, civic participation and democratic process, and privacy and data protection. It is benchmarked against the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the United Nations Guiding Principles on Business and Human Rights, and the Constitution of Bangladesh. We have excluded two legislations, the Competition Act, 2012 and the Consumer Rights Protection Act, 2009, as they primarily concern market competition, consumer protection, and broader economic regulation rather than the protection of the fundamental rights examined in this section. Our analysis of the remaining statutes combines a review of the legislations against the above standards with consultations and interviews involving legal and constitutional experts, civil society representatives, and individuals with direct experience of the legislations' effects, in order to assess both the legal framework and the lived experiences of affected rights-holders. Use of the term "adverse impact" denotes significant or substantial negative influence, effect, or consequence resulting from the legislations on the protection and exercise of the fundamental rights, and this classification includes situations where there is little or no credible evidence of actual harm to date, but where the design or implementation of a legislation creates a significant likelihood of adverse human rights impacts. The classifications are indicative rather than exhaustive and should not be interpreted as definitive assessments of the current human rights impact of the legislation.

LEGISLATIONS	FREEDOM OF EXPRESSION	CIVIC PARTICIPATION AND DEMOCRACTIC PROCESS	PRIVACY AND DATA PROTECTION
Personal Data Protection Act, 2026			
National Data Management Act, 2026			
Cyber Protection Act, 2026			
Bangladesh Telecommunication Act, 2001			
Penal Code, 1860			
Pornography Control Act, 2012			

KEY RECOMMENDATIONS

The recommendations set out below are a non-exhaustive selection drawn from the findings of this white paper, intended to highlight a select few priority areas, and should not be regarded as a substitute for the full set of recommendations contained in the report. These recommendations should therefore be read holistically and in conjunction with the report's broader analysis and findings.

1. ***Amend surveillance and interception protocols, and information disclosure mandates.*** Existing laws on electronic and digital surveillance, interception, and information disclosure need amendments to ensure compliance with domestic and international standards for privacy protection. Activities infringing individual privacy and organizational information security should be subject to robust, independent judicial oversight, ensuring that LEAs are accountable to independent and impartial courts in conducting investigations. Clearer guidelines on data collection, use, transmission, and retention should be adopted to prevent misuse and overreach, with explicit limits on how data collected for specific legal purposes may be stored and shared. At all material times, regulatory transparency must be maintained to ensure accountability and public trust. We recommend enactment of a comprehensive new statute regulating the investigatory powers of LEAs and Intelligence Agencies.

2. ***Introduce new online safety standards and procedures for content regulation.*** Existing laws on online content are inadequate to effectively address harmful online content and should therefore be repealed. Drawing from successful regulatory models in other countries, a new statute should be introduced to address speech-related offenses in alignment with domestic and international standards for free speech. Specifically, non-violent and non-harmful speech should be decriminalized to prevent the misuse of legal provisions to silence journalists, activists, and ordinary citizens, with civil remedies or administrative penalties available for less serious violations where appropriate. Harmful content, such as CSAM and TFSV, should be subject to stricter sanctions. Additionally, the *Cyber Protection Act, 2026* and *Bangladesh Telecommunication Act, 2001* should be substantially amended to enhance the independence of the relevant regulator, empowering it to assess content removal requests based on legal grounds rather than political pressures, ensuring that content regulation upholds democratic discourse. To prevent misuse and ensure fairness, robust procedural safeguards must be integrated into both the new and amended laws.

3. ***Introduce a robust but balanced cybersecurity framework with diverse governance***. Existing laws on cybersecurity are fragmented and inadequate to effectively address non-content technology-enabled crimes and should therefore be substantially amended. Within the current framework, legal mechanisms to counter cybersecurity crimes — including hacking, identity theft, financial fraud, ransomware, unauthorized data modification and access, and other offenses related to digital infrastructure and information and communications technologies — should be strengthened. Furthermore, the governance structure of cybersecurity institutions, particularly the NCPA, should include independent experts, civil society representatives, and data protection specialists to ensure that security measures do not encroach upon civil liberties. An inclusive governance approach would promote transparency, accountability, and public trust, balancing the state's security imperatives with the protection of individual rights.

4. ***Strengthen competition and consumer protection in the digital ecosystem***. The existing competition statute is not fully adapted to the digital economy, enabling technology companies to abuse their dominant position in markets to the detriment of consumers and competitors. Similarly, consumer protection laws are not fully adapted to the digital economy, exposing users to fraud and data vulnerabilities in online transactions. A comprehensive digital competition and consumer protection framework, and a separate e-commerce statute, should be established, incorporating precise and inclusive definitions and extraterritorial provisions, defining standards for e-commerce, privacy in consumer data, and penalties for fraudulent activities, while harmonizing with related laws to avoid conflict of laws. Such reforms would also promote confidence in Bangladesh's digital economy, protecting both consumers and responsible businesses, while encouraging foreign investment.

5. ***Clarify implementation of the Personal Data Protection Act, 2026.*** The government should immediately explain the rationale for the deferral of the *Personal Data Protection Act, 2026* and provide clear guidance regarding compliance expectations, implementation timelines, and transitional arrangements applicable to both public and private sector entities. In particular, executive guidance documents, regulatory roadmaps, phased implementation frameworks, or comparable compliance mechanisms should be issued to assist organizations in preparing for eventual implementation. Absent such clarity, many entities, including small and medium-sized enterprises with limited technical, financial, and compliance resources, may find themselves unable to meet statutory requirements once the legislation enters into force, exposing them to technical non-compliance and potential regulatory penalties despite having had insufficient opportunity to prepare.

6. ***Introduce sentencing guidelines, a recommendation system, and a centralized case-tracking system.*** Currently, there are no structures or systems to ensure balanced and consistent sentencing in criminal cases. Without sentencing guidelines, a recommendation system, and a centralized system for tracking case precedents, judges are left with broad discretion, undermining the fairness and consistency of the sentencing process. Establishing these systems would promote greater uniformity, predictability, and proportionality in the application of penalties, reduce unwarranted sentencing disparities, and minimize the risk of arbitrary outcomes.

A PATCHWORK OF LEGISLATIONS AND SOFT LAWS

CLOSE TO 100 LEGISLATIONS AND SOFT LAWS HAVE DOMINATED DIGITAL GOVERNANCE IN BANGLADESH, SYSTEMICALLY ERODING PRIVACY, FREE SPEECH AND ACCESS TO INFORMATION, AND EXACERBATING MARKET FAILURES.

We provide a non-exhaustive list of legislations below that are relevant to digital governance. Collectively, they have promoted surveillance and unrestricted data access to law enforcement, infrastructure control, censorship, search and seizure of data, devices and assets, without procedural safeguards, and exacerbated market dominance.

Surveillance and Personal Data Access

1. Bangladesh Telecommunications Act, 2001
2. Telegraph Act, 1885
3. Wireless Telegraphy Act, 1933
4. Cyber Protection Act, 2026
5. Personal Data Protection, 2026
6. National Data Management Act, 2026
7. Information and Communication Technology Act, 2006
8. Code of Criminal Procedure, 1898
9. Part IXA, Constitution of Bangladesh
10. Foreign Donations (Voluntary Activities) Regulation Act, 2016
11. Special Powers Act, 1974
12. Anti-Terrorism Act, 2009
13. Money Laundering Prevention Act, 2012
14. Narcotics Control Act, 2018
15. Drugs and Cosmetics Act, 2023
16. National Identity Registration Act, 2010
17. Mobile Court Act, 2009
18. Mutual Legal Assistance in Criminal Matters Act, 2012
19. Foreign Exchange Regulation Act, 1947
20. Bankers' Books Evidence Act, 2021
21. Bank Companies Act, 1991
22. Evidence Act, 1872
23. Representation of the People Order, 1972
24. Statistics Act, 2013
25. Prevention of Corruption Act, 1947
26. Imports and Exports (Control) Act, 1950

Censorship, and Information and Media Control

27. Part III, Constitution
28. Cyber Protection Act, 2026
29. Personal Data Protection, 2026
30. Penal Code, 1860
31. Anti-Terrorism Act, 2009
32. Pornography Control Act, 2012
33. Right to Information Act, 2009
34. Consumer Rights Protection Act, 2009
35. Contempt of Courts Act, 1926
36. Official Secrets Act, 1923
37. Copyright Act, 2023
38. Trademark Act, 2009
39. Patents and Designs Act, 1911
40. Children Act, 2013
41. Mobile Court Act, 2009
42. Bangladesh News Agency Act, 2018
43. Press Council Act, 1974
44. Cinematograph Act, 1918
45. Censorship of Films Act, 1963
46. Printing Presses and Publications (Declaration and Registration) Act, 1973
47. Note-Books (Prohibition) Act, 1980
48. Cable Television Network Management Act, 2006
49. Smoking and Tobacco Products Usage (Control) Act, 2005
50. Drugs and Cosmetics Act, 2023
51. Narcotics Control Act, 2018
52. Representation of the People Order, 1972
53. Code of Criminal Procedure, 1898
54. Bangladesh Telecommunications Act, 2001

Internet Shutdowns and Infrastructure Control

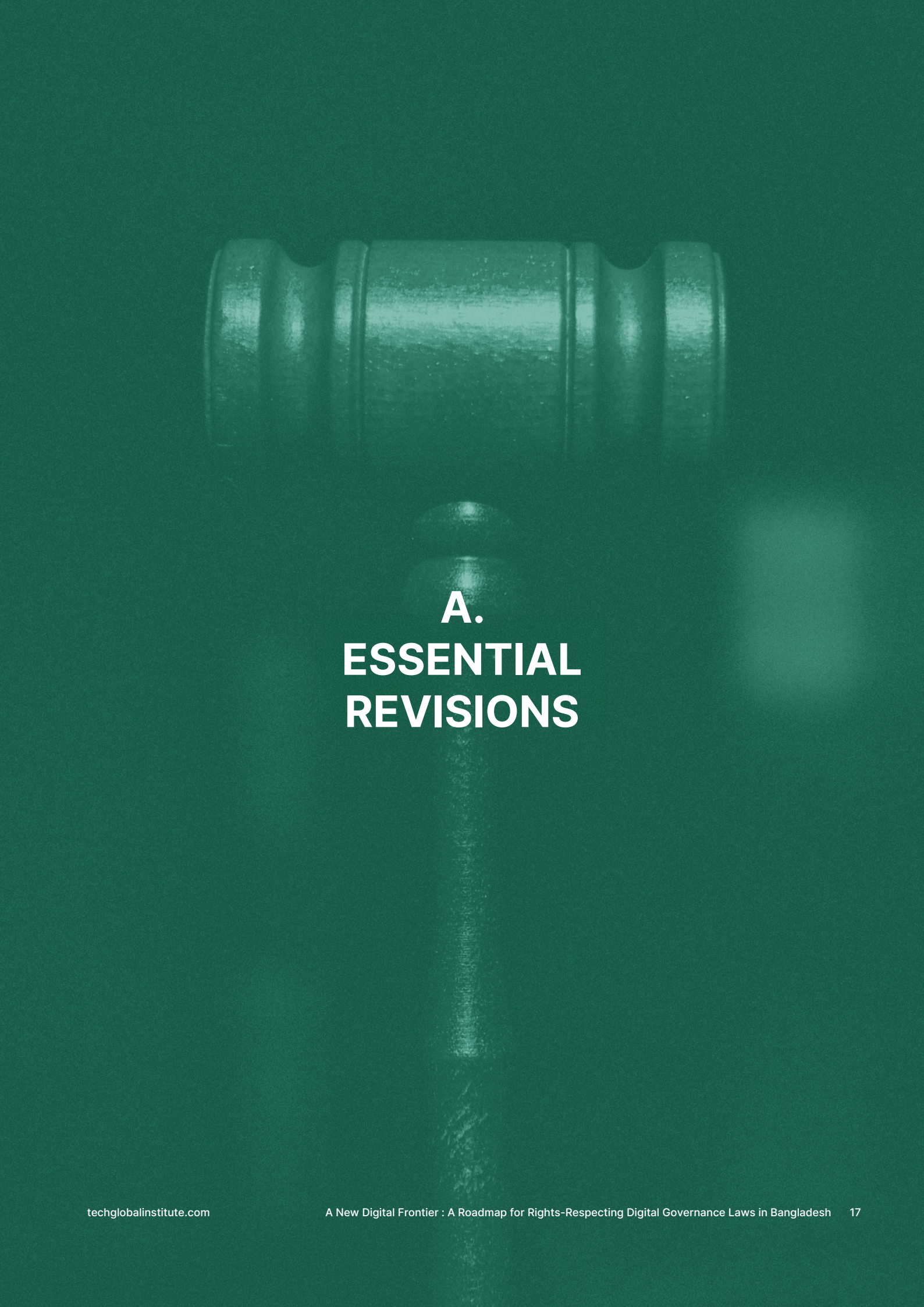
55. Code of Criminal Procedure, 1898
56. Bangladesh Telecommunications Act, 2001

Market Dominance

57. Competition Act, 2012
58. Securities and Exchange Ordinance, 1969
59. Foreign Exchange Regulation Act, 1947
60. Part III, Constitution

Search and Seizure

61. Code of Criminal Procedure, 1898
62. Bangladesh Telecommunications Act, 2001
63. Special Powers Act, 1974
64. Narcotics Control Act, 2018
65. Anti-Terrorism Act, 2009
66. Money Laundering Prevention Act, 2012
67. Prevention of Corruption Act, 1947
68. Cyber Protection Act, 2026
69. National Data Management Act, 2026
70. Information and Communication Technology Act, 2006
71. Customs Act, 1969
72. Mobile Court Act, 2009
73. Explosives Act, 1884
74. Foreign Donations (Voluntary Activities) Regulation Act, 2016
75. Foreign Exchange Regulation Act, 1947
76. Bankers' Books Evidence Act, 2021
77. Statistics Act, 2013
78. Pornography Control Act, 2012
79. Companies Act, 1991
80. Consumer Rights Protection Act, 2009
81. Copyright Act, 2023
82. Patents and Designs Act, 1911
83. Imports and Exports (Control) Act, 1950
84. Special Powers Act, 1974
85. Censorship of Films Act, 1963
86. Note-Books (Prohibition) Act, 1980
87. Smoking and Tobacco Products Usage (Control) Act, 2005
88. Drugs and Cosmetics Act, 2023
89. Narcotics Control Act, 2018
90. Arms Act, 1878
91. Forest Act, 1927
92. Environment Conservation Act, 1995



A. ESSENTIAL REVISIONS

1. Personal Data Protection Act, 2026

The *Personal Data Protection Act, 2026* represents a significant shift in Bangladesh's digital governance landscape by introducing the country's first cross-sectoral data protection framework, moving away from earlier policy proposals centered on data localization, criminal penalties, and expansive punitive enforcement. Now, the statute introduces several positive developments, including recognition of core data subject rights, a comparatively narrower approach to cross-border data transfers, and a more moderate civil penalty framework.

However, across the framework, broad regulatory and executive powers are frequently coupled with undefined legal standards, significant reliance on future regulations and directives, and limited operational guidance. This creates risks of expansive executive discretion and inconsistent enforcement, particularly in Bangladesh's context of evolving regulatory capacity, weak compliance culture, and historically broad use of security- and public-order-related justifications to curtail fundamental rights.

Several substantive concerns emerge across the statute. The exemptions framework under section 24 allows state authorities to invoke broad concepts such as "national security," "public interest," and "public order" to collect vast amounts of personal data without the same compliance requirements as non-state counterparts, risking normalization of expansive state access to personal data without sufficiently robust procedural safeguards, independent oversight, or accountability mechanisms. Similarly, while the provisions provide for a comparatively narrower, notification-based approach to cross-border data transfers, the interoperability and centralized database integration architecture established under the *National Data Management Act, 2026*, with potential obligation to compulsorily store data within national systems, creates significant uncertainty regarding the future direction of cross-border data transfers. The statute also adopts technologically ambitious mechanisms, such as system-wide deletion and propagation obligations, which, if successful, risk being instrumentalized as content-removal mechanisms affecting freedom of expression, press freedom, historical preservation, and public access to information. Additionally, concerns remain regarding the operational independence of the NDMA, broad extraterritorial application without clearly defined jurisdictional thresholds, underdeveloped cybersecurity governance obligations, and a breach-notification framework that relies excessively on subjective assessments that risks underreporting and reduced transparency.

Accordingly, the overall recommendation is not rejection of the framework itself, but substantial amendment through clearer statutory drafting, stronger procedural safeguards, and more independent oversight and accountability mechanisms. More broadly, the recommended reforms seek to ensure that Bangladesh's emerging data governance framework remains rights-respecting and innovation-enabling, while avoiding excessive centralization of state data power, regulatory uncertainty, and disproportionate interference with fundamental rights.

SCOPE AND APPLICATION

Section 1(3) — Deferred commencement

ASSESSMENT

The statute adopts a deferred commencement model, providing an approximately 18-month grace period for six provisions — specifically, section 23 (requiring significant data controllers to appoint data officers) and sections 31 to 35 (penalties for non-compliance) — thereby postponing enforcement, while operationalizing the remaining provisions retrospectively from November 6, 2025. While this approach appears inspired by the EU's GDPR transition model, it suffers from two critical shortcomings.

First, it does not clarify the rationale for the deferral, which has created confusion amongst both state and non-state actors regarding compliance expectations and timelines, nor has there been any executive guidance, regulatory roadmap, or compliance framework issued by the government to assist entities in preparing for implementation. The EU's data protection framework was built over decades of legal, institutional, and jurisprudential development, beginning with the Data Protection Directive 95/46/EC in 1995, reinforced by the *Charter of Fundamental Rights of the European Union* in 2000, and culminating in the adoption of the GDPR in 2016. After its enactment, the GDPR had a transition period between 2016 and 2018, which was supported by a layered ecosystem of extensive guidance, enforcement capacity, and compliance tools, underpinned by strong institutional coordination and regulatory oversight. In contrast, Bangladesh lacks a comparable data protection legacy, institutional readiness, regulatory guidance, or compliance culture, and there has been limited observable progress by the NDMA in the months following its establishment.

Second, the exclusion of the obligation to appoint data officers during the transition period is counterproductive, as such roles are central to enabling organizations to implement governance structures, undertake compliance audits, and embed accountability mechanisms to ensure that systems, processes, and designs are aligned with statutory requirements before the statute comes into effect. As a result, the deferral risks becoming a formal delay without substantive preparedness, undermining both effective implementation and the protection of citizens' data rights.

RECOMMENDATIONS

Amend the provision to require appointment of data officers during grace period, and introduce directives and implementation roadmap.

Establish a clear, phased implementation roadmap supported by guidance. The government, through the NDMA, should clarify the rationale for the grace period and reframe it as an active compliance window, rather than a passive deferral of enforcement. A structured, phased, and proactive approach to implementation should be adopted, with clearly sequenced obligations and timelines aligned with institutional and market readiness. Directives and compliance guidelines should be issued, with clearly defined, phased milestones (e.g., data mapping, risk assessments, contract updates, and governance structures), along with practical guidance on operationalizing core statutory obligations (e.g., consent management, transparency, data protection impact assessments, breach notification, data minimization, and purpose limitation).

For instance, the United Kingdom's *Data (Use and Access) Act 2025* adopts a staged implementation model, bringing different provisions into force at different times through commencement regulations, while Singapore's *Personal Data Protection Act 2012* implemented provisions in phases over specific timelines — allowing regulators and industry to prepare incrementally. For Bangladesh, this approach should be complemented by early issuance of regulatory guidance and alignment with existing frameworks, enabling a smoother transition and reducing compliance burdens, particularly for smaller entities. It should also be supported by sector-specific guidance and toolkits, as well as sustained stakeholder engagement, public updates, consultations, and reporting on implementation progress to reduce uncertainty, raise awareness, and enhance compliance. To enable this, the NDMA should be fully operationalized with adequate resources and a clear mandate to provide oversight, coordinate implementation, and build enforcement readiness, ensuring that the transition period results in substantive preparedness rather than formal delay.

Amend the provision to require mandatory appointment of data officers during grace period. The requirement to appoint data officers under section 23 should be brought into effect earlier to ensure organizations can meaningfully prepare by building internal governance structures, conducting audits, and aligning systems with statutory requirements. Comparative practice supports this approach. For instance, under the EU's GDPR, obligations relating to data protection officers were applicable from the effective date and were widely treated as foundational compliance steps during the transition period. Similarly, Brazil's *General Law on the Protection of Personal Data 2019* and Singapore's *Personal Data Protection Act 2012* required the designation of a data protection officer early in the compliance cycle. Establishing internal accountability structures at an early stage is critical to enabling effective compliance, even where enforcement of penalties is phased or delayed.

Sections 1(2), 1(3), 4(1), 4(2) — Extraterritorial application

ASSESSMENT

Overbroad extraterritorial application under the statute creates legal uncertainty, risks of jurisdictional overreach, and potential conflicts with foreign legal regimes, particularly for cross-border digital services and data flows. Specifically:

(i) Application of the statute is extended under section 1(2)(c) to any person or entity processing personal data outside Bangladesh where such processing is connected to offering services to, or monitoring, individuals located in Bangladesh. While aligning in part with global data protection approaches, the provision lacks clear thresholds (e.g., targeting, scale, intent, or business size), thereby likely capturing a wide range of incidental or minimal interactions with Bangladeshi users, and creating uncertainty for foreign entities with limited or indirect nexus to the jurisdiction.

(ii) Extraterritorial jurisdiction, under section 4(1) and (2), extends the application of the statute to both Bangladeshi citizens committing offenses abroad as well as any person outside Bangladesh whose conduct has effects within Bangladesh, treating both such acts as if they were committed domestically. These provisions are broadly framed and, in the absence of limiting principles or comity-based safeguards, may enable expansive assertions of jurisdiction over non-resident citizens and non-nationals, including those without

physical presence or meaningful operational control within Bangladesh. It also leaves the question of assessing citizenship and establishing jurisdictional nexus in cross-border digital contexts unclear, particularly where individuals may hold dual nationality, operate through decentralized digital infrastructures, or engage in activities across multiple jurisdictions.

When read together, these provisions create a sweeping extraterritorial framework that extends regulatory obligations and liability across cross-border data processing, without ensuring commensurate protection of citizens' privacy and data rights. Although similar provisions exist in comparable legislations, such as EU's GDPR, they are accompanied by a high degree of institutional readiness, coordinated enforcement mechanisms, regulatory guidance, and an established compliance culture — conditions that do not appear to be present in Bangladesh, as noted above. From a practical standpoint, enforcement is likely to face significant challenges, including difficulties in asserting jurisdiction over foreign entities without local presence, limitations in cross-border regulatory cooperation, and constraints in investigating, sanctioning, or ensuring compliance by actors operating across multiple jurisdictions. Absent clear and enforceable jurisdictional thresholds, safeguards against duplicative enforcement, or mechanisms for international cooperation, the risks of fragmented compliance and inconsistent application is heightened. From a rights perspective, this overbroad and uncertain scope may undermine legality and due process, expose individuals and entities to unpredictable liability, and weaken effective protection of the right to privacy by prioritizing jurisdictional reach over substantive safeguards and accountability.

RECOMMENDATIONS

Amend the extraterritoriality provision and develop cross-border enforcement and cooperation mechanisms.

Amend the provision to clarify and limit the scope of extraterritorial application through defined jurisdictional thresholds. The statute should be amended to introduce clear and objective criteria for extraterritorial applicability, such as demonstrable intent to target the Bangladeshi market, a minimum threshold of user base or business activity, and a requirement of substantial connection (or nexus) to Bangladesh. Criteria should be defined based on scale, nature of processing, and business size to avoid capturing incidental or low-risk interactions. Additionally, section 4 should be refined to incorporate limiting principles grounded in international comity, including clearer standards for establishing jurisdiction, safeguards against duplicative or parallel proceedings, and clarification on applicability to dual nationals and cross-border digital actors. Comparative approaches illustrate how such thresholds can be structured: under EU's GDPR, extraterritorial application is tied to "offering goods or services" or "monitoring behaviour" within the EU, interpreted through clear targeting criteria. At the same time, judicial interpretation by the Court of Justice of the European Union has further clarified the limits on expansive assertions of jurisdiction in *Google Inc. v. Commission nationale de l'informatique et des libertés*, noting that obligations under the GDPR do not automatically extend to global enforcement. Similarly, India's *Digital Personal Data Protection Act, 2023* applies to processing outside India only where it is in connection with offering goods or services to individuals in India. Meanwhile, the *California Consumer Privacy Act of 2018* applies the law based on business size and data volume thresholds, such as annual revenue (e.g., US$ 25,000,000), number of consumers and households processed (e.g., 100,000+), or percentage of revenue derived from selling data.

Develop a coordinated framework for cross-border enforcement and cooperation. To operationalize the extraterritorial scope, the statute should align with global standards for cross-border data flows, and the government should establish mechanisms for

international regulatory cooperation, including mutual legal assistance arrangements and data transfer frameworks (e.g., adequacy-type assessments or equivalent safeguards). Comparative approaches illustrate different models: under the EU's GDPR, cross-border enforcement is supported by a structured cooperation and consistency mechanism among supervisory authorities, alongside adequacy decisions and standardized legal mechanisms such as pre-approved contractual clauses and corporate rules to facilitate cross-border data flows; Brazil's *General Law on the Protection of Personal Data 2019* enables international data transfers through adequacy and contractual safeguards while empowering the regulator to engage in cooperation with foreign counterparts. This should be complemented by detailed regulatory guidance clarifying compliance expectations for foreign entities, as well as procedural safeguards to ensure due process and consistency in enforcement. Strengthening institutional capacity and coordination in this manner would mitigate enforcement challenges, reduce fragmentation, and ensure that the exercise of extraterritorial jurisdiction supports, rather than undermines, effective protection of privacy and data rights.

Section 24 — Exemptions

ASSESSMENT

The statute exempts consent and other permissible mechanisms for processing personal data on certain grounds, including national security, defence, public order, public interest, and the prevention, detection, investigation, or prosecution of crimes. At the same time, sub-sections (2), (4), and (5) seek to preserve certain safeguards by clarifying that other data protection obligations continue to apply, restricting exemptions where they create disproportionate impacts on rights and freedoms or lack legal authority or necessity, and empowering the NDMA to review misuse of exemptions. On its face, this framework broadly resembles approaches adopted in modern data protection regimes, including the GDPR, which also recognizes limited grounds for processing without consent in matters relating to public interest and law enforcement.

However, the operation of these provisions should be assessed within Bangladesh's broader institutional and governance context. The breadth and vagueness of terms such as "public interest," "public order," and "national security" have historically been used to justify rights-infringing conduct, including surveillance and interception; and, combined with the absence of detailed statutory thresholds, procedural clarity, and robust independent oversight, they creates significant scope for expansive interpretation and discretionary application. From a practical standpoint, these exemptions risk legitimizing and normalizing broad forms of state access to personal data and surveillance activities under generalized security or public interest justifications, especially in a system characterized by concerns regarding strong executive influence, weak oversight, limited transparency, and insufficient institutional accountability. Without sufficient guardrails embedded in the statute addressing these concerns, exemptions intended to be exceptional may become normalized and discretionary, creating risks of arbitrary and disproportionate interference with fundamental rights, including privacy, freedom of expression, and freedom of association, especially in politically sensitive contexts.

RECOMMENDATIONS

Amend the exemptions provision.

Amend the provision to embed additional procedural guardrails to ensure that exemptions are exercised in a transparent, necessary, and proportionate manner. The statute should incorporate stronger procedural and institutional safeguards as positive legal obligations governing the use of exemptions. Specifically, this should include mandatory statutory obligations to conduct written necessity and proportionality assessments prior to reliance on exemptions, in statutorily prescribed formats and shared with the NDMA; mandatory statutory obligations to maintain comprehensive audit trails and records of decisions; and publication of periodic transparency reports containing aggregated information on the use of exemptions, categories of data processed, and the legal bases invoked, subject only to narrowly tailored confidentiality limitations. The law should also establish formal cross-party parliamentary oversight mechanisms, including periodic reporting to and review by a parliamentary committee, alongside powers for the NDMA to conduct independent audits and publish findings. Additionally, affected individuals should have access to effective complaint and redress mechanisms, including the ability to challenge unlawful or disproportionate reliance on exemptions before an independent body or court. Each of these safeguards should be clearly articulated in sufficient detail within the statute itself to ensure direct enforceability and prevent reliance on broad executive discretion.

Comparable safeguards exist in other jurisdictions. For instance, the United Kingdom's *Investigatory Powers Act 2016* embeds statutory requirements of necessity and proportionality assessment, structured, multi-layered ("double lock") authorization procedures involving both executive and judicial branches, mandatory recordkeeping and audit obligations, annual transparency reporting with statistics on warrants, safeguards, and errors to parliament, and independent oversight by both judicial commissioners and parliamentary committees such as the Intelligence and Security Committee of Parliament. Such frameworks demonstrate that broad state access powers can be accompanied by enforceable procedural safeguards, institutional accountability, and transparency obligations embedded directly within legislation, rather than left to executive discretion or post facto policy development.

DATA RIGHTS

Section 5, 7, 9 — Consent and exceptions, children's data

ASSESSMENT

Consent is one of the central mechanisms for lawful collecting and processing citizens' data, yet the provisions create a broad set of alternative lawful bases permitting processing without consent, with special provisions for children. Specifically:

(i) Alternative lawful bases permitting processing without consent includes, sections 5(3) and 7(b) to (f), contractual necessity, establishment or exercise of legal rights, protection of vital interests relating to life or health, and performance of duties imposed by law. On its face, this framework broadly aligns with modern data protection regimes. However, the breadth of the non-consensual processing grounds, combined with the absence of detailed statutory thresholds and operational safeguards, has the effect of diluting the practical role of consent as a meaningful

mechanism of user autonomy and control. Especially in Bangladesh's broader institutional context, characterized by weak compliance and enforcement culture, limited regulatory capacity, low levels of public awareness regarding data rights, and concerns regarding executive influence and accountability deficits, there is a heightened risk that these exceptions may become normalized rather than exceptional, and used to bypass the consent mechanism. Without stronger guardrails, data subjects may formally retain rights while lacking practical ability to exercise meaningful control over how their personal and sensitive data are collected, processed, shared, and retained.

(ii) A special regime governing the processing of personal data of children and persons incapable of giving consent is established in section 9, allowing processing based on parental or guardian consent; it also requires consideration of the rights and interests of such persons, and prohibits behavioral tracking, profiling, and targeted advertising directed at them. While these protections broadly reflect emerging international standards relating to children's privacy and online safety, the framework remains operationally underdeveloped — it does not clarify how parental or guardian consent is to be given or verified, how the age or evolving capacity of individuals will be assessed, or how data controllers are expected to transition from parental consent to direct consent once the data subject reaches adulthood or otherwise attains capacity to consent. Specifically, the provision allowing parental consent to remain valid until the child turns 18 risks creating long-term processing arrangements without a clear mechanism for renewed, informed consent from the now-adult data subject. Comparable age-assurance and age-gating frameworks in other jurisdictions have similarly faced implementation challenges: for example, Australia's *Online Safety Amendment (Social Media Minimum Age) Act 2024* and the United Kingdom's *Online Safety Act 2023* have raised concerns regarding operational and enforcement feasibility, as children may misreport their age, borrow adult accounts or devices, rely on anonymity, or otherwise bypass verification tools. On the other hand, operationalizing such provisions effectively would likely require collection of sensitive identity, biometric, or behavioral data, and, without accompanying safeguards such as strict data minimization, purpose limitation, retention restrictions, independent oversight, and privacy-preserving age assurance mechanisms, may itself generate additional privacy and surveillance risks, thereby becoming counterproductive to the intended protective objective of the provision.

RECOMMENDATIONS

Amend consent and children's data right provisions.

Amend the provision to strengthen consent safeguards and narrow alternative lawful processing grounds. The statute should more clearly define alternative lawful bases for processing, and explicitly require them to be narrowly interpreted, to ensure that consent remains the primary mechanism for lawful data processing, rather than becoming functionally optional. Specifically, the law should require data controllers to document and justify reliance on alternative lawful bases through mandatory necessity and proportionality assessments, maintain records of the lawful basis relied upon, and provide clear notice to data subjects identifying the specific ground for processing. With respect to necessity and proportionality assessments, the statute (or a secondary legislation) should define the applicable criteria and methodology, including assessment of the legitimacy of the objective pursued, the necessity of processing to achieve that objective, availability of less intrusive alternatives, proportionality of the data processing in relation to the intended purpose, categories and sensitivity of data involved, duration of retention, risks to rights and freedoms of data subjects, and mitigation measures adopted by the controller. Additional safeguards should apply to sensitive personal data, including mandatory data protection impact assessments for high-risk processing,

stricter purpose limitation and retention requirements, and enhanced oversight and audit powers by the NDMA. The statute should also clarify, through illustrations and explanations, that grounds such as "voluntary public disclosure" or "protection of vital interests" must be interpreted narrowly and cannot be relied upon to justify broad or unrelated secondary uses of personal data.

Comparable approaches exist in other jurisdictions: under the GDPR, similar provisions require processing to be limited to specified lawful bases and subject to principles such as purpose limitation and data minimization, while imposing heightened safeguards and mandatory data protection impact assessments for high-risk or sensitive data processing. Similarly, South Africa's *Protection of Personal Information Act 2013* requires processing to be "adequate, relevant and not excessive" in relation to the purpose pursued, restricts incompatible secondary processing, affords special personal information additional protections and structured exemptions under, and requires prior authorization from the regulator for certain categories of high-risk processing.

Operationalize children's data protections through clear statutory safeguards and age-appropriate governance measures. Either amend the statute or formulate rules to establish detailed and enforceable requirements for processing children's data, including specific provisions on verifiable parental consent mechanisms proportionate to the level of risk involved, periodic revalidation of parental consent, and mandatory transition procedures requiring renewed consent directly from the data subject upon reaching the age of majority or attaining capacity to consent. Data controllers should also be subject to heightened privacy-by-design obligations, including strict data minimization, default high privacy settings, restrictions on retention, sharing and secondary use of children's data. Additionally, the NDMA should be empowered to issue binding technical standards and codes of practice on age assurance, parental verification, and privacy-preserving verification mechanisms to ensure that implementation does not itself create disproportionate privacy or surveillance risks.

Comparable safeguards can be found in the United Kingdom's Age Appropriate Design Code, which requires high privacy settings by default, data minimization, and restrictions on profiling and geolocation for children. Likewise, the United States' *Children's Online Privacy Protection Act of 1998* and *Children's Online Privacy Protection Rules of 2013* require verifiable parental consent and impose obligations relating to notice, retention, and use limitations for children's data. More recently, legislative proposals such as the *Kids Online Safety Bill* have emphasized heightened duties of care for online platforms in relation to minors, including stronger safeguards against harmful design features, enhanced privacy protections, default safety settings, and limitations on profiling and targeted recommendations for children, reflecting growing recognition that children's data requires heightened and ongoing protections extending beyond initial collection and consent.

Sections 12, 13, 14 — Right to rectification, updating, and deletion, and its system-wide propagation

ASSESSMENT

A broad framework for rectification, updating, withdrawal of consent, objection to processing, deletion of personal data, and their system-wide propagation across interconnected databases and systems, while potentially necessary for strengthening individuals' autonomy and control over their personal data, in its current formulation risks being instrumentalized as a content alteration or removal mechanism. Particularly, section 13(2) creates a substantive right to deletion on broad grounds, such as purpose limitation, consent withdrawal, unlawful processing, or data subject objection, while section 14 attempts to operationalize these rights by requiring approved changes and deletions to propagate across primary and secondary

databases, including mirrored systems, backups, caches, disaster recovery environments, and migration datasets.

On its face, this broadly resembles the "right to erasure" or "right to be forgotten" recognized in comparable data protection regimes such as the GDPR. However, the framework adopted here is unusually expansive and technologically ambitious, raising concerns regarding implementation feasibility, institutional readiness, cybersecurity, and risks of misuse, especially in Bangladesh's context of weak institutional coordination and inadequate accountability safeguards. From a technical standpoint, implementing accurate, system-wide deletion across interconnected systems, archived environments, caches, and immutable infrastructures is inherently difficult, resource-intensive, and susceptible to inconsistency and over-removal.

More broadly, the framework risks functioning as a content regulation mechanism rather than remaining confined to data protection. In digital environments, there is often an unavoidable conflation between "data" and "content": personal data is frequently embedded within journalistic reporting, social media posts, public records, search engine indexing, audiovisual material, and other forms of expression. As a result, exercising erasure rights may, in practice, directly affect the accessibility, visibility, or continued existence of lawful public-interest online content. Comparative experience in Europe demonstrates this tension: the right to be forgotten gained prominence following the decision of the Court of Justice of the European Union in *Google Spain SL and Google Inc. v AEPD and Mario Costeja González*, where González sought to remove access to embarrassing online information about him from search engines. Although framed as a "right to erasure," the court ultimately adopted a narrower approach centered on de-prioritization in search engine results, rather than deletion of the underlying content itself, reflecting an attempt to balance privacy rights with freedom of expression and press freedom. Subsequently, the European framework evolved through jurisprudence and regulatory practice to incorporate stronger balancing principles, thereby limiting the use of erasure rights as broad censorship mechanisms. In contrast, Bangladesh's more literal and formalistic interpretive culture — combined with concerns regarding executive influence, weak institutional safeguards, and politicized enforcement environments — creates heightened risks that erasure powers could be invoked by politically exposed persons, corporations, or other powerful actors to suppress lawful information of public interest, erase historical records, or pressure intermediaries and media platforms into removing critical or embarrassing material. From a human rights perspective, such risks directly implicate freedom of expression, press freedom, the public's right to receive information, historical memory, and democratic accountability, particularly where removal requests concern matters of corruption, political conduct, public office, or other issues legitimately subject to public scrutiny.

RECOMMENDATIONS

Amend erasure right and system-wide propagation provisions.

Amend the erasure and system-wide propagation framework to incorporate stronger substantive and procedural safeguards against overbroad removal and abuse. The statute should clearly define what deletion means, which could include a range of measures from actual removal to de-indexing, restriction of processing, geo-blocking, annotation or contextualization of disputed information, controlled or limited access, and anonymization or pseudonymization; each of these terms should be clearly defined and explained through illustrations. Additionally, the statute should also expressly require that erasure-related provisions be interpreted narrowly and contextually, balanced against competing rights and public interests, including freedom of expression, press freedom, journalistic activity, historical preservation, academic research, and the public's right to access information. Where, for example, requests involving matters of public interest — such as political activities, public office, corruption,

criminal proceedings, corporate misconduct, or journalistic reporting — are involved, they should be subject to heightened scrutiny, including mandatory constitutionally mandated necessity and reasonableness assessments, and opportunity for independent review before any removal or propagation order is issued. To effectively operationalize the provision, it should also require reasoned written decisions and maintain transparency obligations through publication of anonymized aggregate statistics on removal requests, process, rationale, and outcomes.

Additionally, the law should clarify the technical scope and limitations of system-wide propagation obligations, including clear criteria and guidance on deletion from archival, backup, integrity-preserving, or immutable systems where less intrusive alternatives — such as restriction of processing, de-indexing, annotation, or controlled access — are available and proportionate. Comparative approaches, especially in Europe, demonstrate that erasure rights should operate within a structured balancing framework that protects both privacy and freedom of expression, rather than functioning as generalized content removal mechanisms.

Section 20 — Personal data security breach

ASSESSMENT

Under the existing framework, obligation to report data breach to the NDMA is only required where the breach is likely to cause significant damage to data subjects, which raises two concerns. First, the framework adopts a likelihood- and damage-based threshold, meaning that the mere occurrence of a breach is insufficient to trigger mandatory reporting obligations; instead, the entity must assess and demonstrate that the breach has caused, or is likely to cause, significant harm to affected individuals. From a practical standpoint, this is an inherently speculative exercise, particularly at the early stages of breach discovery where the scope, downstream consequences, and exploitability of compromised data may remain unclear. Secondly, in assessing the significance or substantiality of breaches, the statute directs consideration of factors such as the nature of the breach, categories and approximate number of affected individuals and information, and remedial measures undertaken by the data controller or processor. However, the framework's reliance on the undefined and subjective threshold of "significant" creates ambiguity regarding when notification obligations are triggered. Collectively, these concerns create substantial discretion for data controllers and processors to determine whether breaches warrant disclosure, and in doing so, to underreport or avoid disclosure of breaches by narrowly interpreting whether harm is sufficiently "significant," thereby weakening transparency, accountability, and effective protection of citizens' data rights.

Illustratively, recent data breach incidents involving entities such as the Office of the Registrar General, Birth & Death Registration (~50 million records) and Shwapno (~4 million records) involve exposure of large volumes of personal and identity-related information affecting potentially millions of individuals, and would likely satisfy even a restrictive interpretation of "significant" damage. However, the current formulation creates uncertainty for smaller-scale breaches — for example, breaches affecting several hundreds, thousands, or tens of thousands of citizens — which may nonetheless expose individuals to identity theft, financial fraud, phishing, surveillance, reputational harms, or other downstream risks. Given Bangladesh's broader context of weak compliance culture, patterns of selective interpretation and enforcement by state institutions, limited regulatory capacity, absence of mature cybersecurity governance frameworks, and incentives to avoid reputational or political accountability, the absence of mandatory reporting requirements for all data breach incidents, or at least objective statutory thresholds and mandatory

reporting criteria, risks systematic underreporting, delayed disclosure, and reduced transparency. This undermines not only effective regulatory oversight and cybersecurity preparedness, but also the ability of affected individuals to take protective measures in response to breaches involving their personal data.

RECOMMENDATIONS

Amend data breach notification provisions.

Amend the breach notification framework to establish clearer, objective, and mandatory reporting obligations. The statute should define reportable data breaches either as (a) an absolute reporting requirement irrespective of the nature or scale of the breach, or (b) a threshold-based model grounded in a combination of objective quantitative and clearly defined qualitative criteria. Either way, it should move away from its current formulation that relies primarily on subjective elements such as the "likelihood" of "significant" damage, as well as a damage-based assessment model, as such harms are often difficult to predict, prove, or enforce against in practice, particularly given existing regulatory and institutional constraints.

An absolute reporting model is preferable in the Bangladeshi context, as it minimizes discretion afforded to data controllers and processors in determining whether a breach satisfies a reporting threshold, thereby reducing risks of underreporting, delayed disclosure, and selective interpretation. This would broadly align with the GDPR, which mandates notification of all personal data breaches, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons — although the latter qualification is not recommended here, as it reintroduces uncertainty and discretionary interpretation. Similarly, Singapore's *Cybersecurity Act 2018* and Australia's *Security of Critical Infrastructure Act 2018* impose mandatory incident reporting obligations for critical information infrastructure breaches within statutory timelines, irrespective of demonstrable harm or damage.

However, if a threshold-based approach is retained, the criteria should be narrowly and objectively defined. Objective indicators could include the categories and sensitivity of data affected, scale of exposure, involvement of children's or sensitive personal data, risks of identity theft, fraud, or misuse, and broader cybersecurity implications. For instance, Singapore's *Personal Data Protection Act 2012*, read with *Personal Data Protection (Notification of Data Breaches) Regulations 2021*, requires notification where a breach is likely to result in significant harm or affects 500 or more individuals, while Australia's *Privacy Act 1988* under the notifiable data breaches scheme, requires notification where unauthorized access, disclosure, or loss is likely to result in "serious harm," supplemented by regulatory guidance identifying objective assessment factors such as the sensitivity of data and likelihood of misuse.

Additionally, the statute or secondary legislation should also prescribe structured breach assessment methodologies, mandatory documentation and recordkeeping obligations, statutory reporting timelines, and standardized reporting formats to reduce discretionary interpretation by data controllers and processors.

CROSS-BORDER DATA TRANSFER

Section 29 — Cross-border data transfer

ASSESSMENT

Over the past several years, policy proposals have gradually evolved from hard localization requirements, to mirroring obligations requiring domestic copies of data, and now toward a narrower, notification-based framework for cross-border transfers of "large amounts" of sensitive personally identifiable data. While this is comparatively more proportionate, the framework still leaves several core concepts insufficiently defined. Specifically, the explanation to section 29(6) links regulation of cross-border transfers to risks involving "national sovereignty," "national security," and "financial stability," but these terms remain broad, politically sensitive, statutorily undefined, and jurisprudentially underdeveloped. Similarly, the requirement that notification obligations apply only to "large amounts" of sensitive personally identifiable data lacks objective thresholds or measurable standards. Collectively, these ambiguities create uncertainty regarding compliance obligations and confer broad interpretive discretion on both regulators and regulated entities.

However, the broader framework under the *National Data Management Act, 2026* creates significant uncertainty regarding the future direction and practical operation of cross-border data transfers. In particular, sections 30(6), 31 and 32 of this statute empowers NDMA to to mandate integration of databases into the national interoperability framework and, where deemed expedient, require compulsory storage of such databases within national database systems. At the same time, section 31 creates a broad and open-ended category of "nationally important / sensitive data," subjecting its management, exchange, and sharing to potential restrictions imposed by the government. Moreover, section 27 empowers the NDMA to issue mandatory orders, directives, advisories, and instructions relating to data governance and management. Read together, these provisions create a framework through which broad executive and regulatory powers may indirectly condition, restrict, or localize cross-border data flows through subordinate regulations, directives, interoperability requirements, or data-classification measures, notwithstanding the comparatively narrower formulation currently reflected in section 29(6) of the *Personal Data Protection Act, 2026*. In practice, this creates significant regulatory uncertainty and unpredictability for cross-border digital services, cloud infrastructure providers, and international data-processing operations, while also raising concerns regarding selective enforcement, discretionary restrictions on information flows, and potential fragmentation of Bangladesh's digital economy from globally interconnected digital and cloud ecosystems. From a human rights perspective, such broad and discretionary powers may facilitate greater centralization of citizens' personal data within state-linked systems, increasing risks of surveillance expansion, profiling, unauthorized secondary use, and function creep beyond the purposes for which data were originally collected.

RECOMMENDATIONS

Amend cross-border data transfer frameworks, and delete all direct or indirect localization provisions.

Amend the framework, or adopt a regulation under section 29(7), to establish clear, objective, and risk-based criteria governing cross-border transfers of sensitive personally identifiable data. The regulations should define key terms such as "national sovereignty," "national security," "financial stability," and "large amounts" through narrowly tailored and measurable standards, including sector-specific thresholds, categories of affected data, scale of transfer, sensitivity of information, and contextual risk factors. Furthermore, notification obligations should be supplemented by structured compliance procedures, including standardized reporting formats, risk assessment methodologies, and documentation requirements.

Comparative approaches illustrate more structured models for regulating cross-border data transfers. Under the GDPR, cross-border transfers are governed through adequacy assessment mechanisms, standard contractual clauses, binding corporate rules, and risk-based safeguards. Singapore's *Personal Data Protection Act 2012*, read with *Personal Data Protection Regulations 2021* and other regulatory guidance, permits international transfers where organizations ensure comparable protection standards through contractual or legal mechanisms, supplemented by detailed regulatory guidance. Bangladesh should similarly adopt a transparent, narrowly tailored, and interoperability-oriented framework that protects sensitive data without creating disproportionate barriers to cross-border digital activity or conferring excessive regulatory discretion or burden on regulators and regulated entities.

[See our recommendation on sections 30(6), 31 and 32 of the National Data Management Act, 2026 below.]

PENALTIES AND COMPENSATION

Sections 31, 32, 33, 34, 35 — Civil penalties

ASSESSMENT

As currently framed, the penalty framework reflects a notable shift from earlier drafts of the legislation, as well as the *Personal Data Protection Ordinance, 2025*, which had sanctions including imprisonment, penal fines, and civil penalties linked to a percentage of business revenue (ranging between 1-2% of annual turnover). However, the present formulation adopts a more predictable and comparatively moderate administrative penalty regime, imposing fines of up to BDT 2,500,000 for general violations and up to BDT 5,000,000 for significant data controllers. This transition moves away from overly punitive criminalization and recognizes the economic realities of Bangladesh's digital ecosystem, where criminal liability or substantial civil penalties could have imposed disproportionate burdens on startups, small businesses, and emerging technology enterprises with limited compliance or financial capacity. While the current approach provides greater legal certainty and business predictability within the liability framework, however:

(i) It appears that the framework assumes that fixed administrative fines alone will produce sufficient deterrent and corrective effects, without establishing a more structured and graduated enforcement architecture. While sections 32 and 33 authorize imposition of administrative penalties for violations of data subject rights and failures in data protection and security, the statute contains limited provisions empowering

the NDMA to impose broader corrective measures such as mandatory compliance orders, suspension of processing, independent audits, remediation plans, deletion or restriction orders, or mandatory security improvements. As a result, the framework risks functioning primarily as a monetary penalty system rather than a comprehensive regulatory compliance regime designed to prevent recurrence of violations and improve data governance practices. This is particularly problematic in Bangladesh, where, with some exceptions (such as multinational corporations), many large businesses remain family-owned and -operated, with weak corporate governance, and limited systems, processes, and design-based compliance embedded into their internal structures. As a result, compliance even in more established regulatory domains — such as labor law, securities regulation, regulatory filings, and licensing compliance — is often treated as secondary, while widespread systemic non-compliance and constrained enforcement capacity may reproduce a legacy of weak implementation even where the statutory framework may be formally sound.

(ii) A relatively low ceiling of civil penalties may be inadequate in addressing systemic or large-scale violations by major multinational technology corporations and other data-driven businesses and digital platforms, whose revenues and data-processing operations operate at significantly larger scales. In such contexts, the fines may have little meaningful deterrent or corrective effect, rendering non-compliant behavior an economically tolerable cost of business. Conversely, a purely turnover-based penalty model without contextual safeguards may also disproportionately burden smaller enterprises and discourage innovation in an emerging digital economy. The current framework therefore risks under-deterring large actors while remaining structurally disconnected from the scale, gravity, and economic realities of different categories of regulated entities.

(iii) The compensation framework under section 35, read with section 44 of the *National Data Management Act, 2026*, relies heavily on the discretion of the NDMA without establishing clear statutory guidance, baseline principles, or structured criteria for determining compensation. The statute does not clearly articulate how economic and non-economic harms — such as distress, reputational injury, loss of autonomy over personal data, or long-term risks arising from data exposure — are to be assessed or quantified, potentially resulting in inconsistent and unpredictable outcomes for affected data subjects.

(iv) An important accountability safeguard present in section 47 of the *Personal Data Protection Ordinance, 2025* and section 53 of the *National Data Management Ordinance, 2025* has been removed. The earlier framework expressly contemplated administrative sanctions against government agencies, statutory bodies, autonomous institutions, and their personnel for violations. In the current statutes, however, this provision has been omitted, while section 24 simultaneously provides broad exemptions for certain government agencies. Read together, these changes risk creating a significant accountability gap whereby some of the largest holders and processors of citizens' personal data may effectively remain insulated from meaningful regulatory consequences and accountability. For example, one report demonstrates how senior officers from specialized policing units improperly accessed "extremely sensitive information" through national intelligence-sharing infrastructure outside their authorized remit, and subsequently shared such data through intermediaries on encrypted messaging platforms for financial gain. Given the scale and sensitivity of personal data routinely processed by state institutions, the absence of a clearly articulated enforcement and penalty framework applicable to public bodies and their personnel may weaken deterrence, reduce incentives for institutional compliance, and undermine public trust in the legitimacy, neutrality, and universality of the data protection regime.

RECOMMENDATIONS

Amend the penalty regime and establish a clearer compensation framework.

Adopt a more structured, graduated, and corrective enforcement framework combining proportionate penalties. The statute should supplement administrative fines with a wider range of corrective and supervisory measures, including mandatory compliance orders, remediation plans, independent audits, temporary suspension or restriction of processing, mandatory security improvements, and recurring penalties for continued non-compliance. Moreover, penalties should also be calibrated through a tiered framework that takes into account the scale of the violation, sensitivity of affected data, duration and intentionality of the misconduct, prior compliance history, and size and turnover of the regulated entity, thereby ensuring proportionality for smaller businesses while preserving meaningful deterrence for large digital platforms and multinational corporations. Such an approach would better reflect Bangladesh's economic and regulatory realities by avoiding disproportionately punitive burdens on startups and emerging enterprises with limited compliance capacity, while simultaneously ensuring that penalties imposed on large domestic and multinational corporations are sufficiently dissuasive, proportionate, and capable of producing meaningful corrective effects. The objective should be to avoid both under-deterrence and over-penalization by embedding proportionality, scalability, and contextual assessment directly within the enforcement architecture.

Comparable jurisdictions adopt a more structured penalty framework, with either substantially higher fixed administrative penalties or turnover-based models linked to revenue, or both. For instance, the GDPR imposes fines of up to €20,000,000 or 4% of total worldwide annual turnover, whichever is higher, alongside the authority to issue warnings, reprimands, processing bans, suspension orders, and compliance directives. Similarly, Brazil's *General Law on the Protection of Personal Data 2019* authorizes fines of up to 2% of the revenue generated from Brazil in the previous year, excluding taxes, capped at R$ 50,000,000 per infringement, together with corrective measures such as public disclosure of violations, blocking or deletion of personal data, and partial suspension of database operations. Australia's *Privacy Act 1988* allows civil penalties for serious or repeated interferences with privacy, with maximum penalties for corporations reaching the greater of A$ 50,000,000, three times the benefit obtained, or 30% of adjusted turnover during the relevant period, supplemented with enforceable undertakings, compliance assessments, and regulatory directions issued by the privacy regulator.

Establish a clearer and more structured statutory compensation framework. While the current formulation empowers the NDMA to award compensation, the statute does not clearly define the methodology for determining compensation, nor does it establish indicative lower or upper limits, baseline principles, or structured criteria for quantification. As such, the statute should explicitly address these factors for assessing compensation, including not only economic but also non-economic harms such as distress, humiliation, reputational injury, loss of control over personal data, identity theft risks, surveillance-related harms, and long-term consequences arising from exposure of personal information. Rather than leaving compensation almost entirely to broad administrative discretion, the law should provide clearer statutory guidance on factors relevant to quantification, while preserving flexibility for context-specific assessment in serious cases.

Comparative approaches provide useful models. For instance, in Australia, the compensation framework for the new tort of serious invasion of privacy in Schedule 2 to the *Privacy Act 1988* recognizes non-economic harms, with references to benchmarks such as "the greater of (c) $478,550; and (d) the maximum amount of damages for non-economic loss that may be awarded in defamation proceedings under an Australian law," thereby introducing some degree of consistency and proportionality in assessing intangible harms. However, pegging compensation to other doctrinal areas such as defamation may itself create additional legal uncertainty in Bangladesh, where jurisprudence relating to non-economic and dignitary harms remains comparatively underdeveloped and inconsistently applied. California

adopts a more structured statutory-damages model: under the *California Consumer Privacy Act of 2018*, statutory damages ranging from US$ 100 to US$ 750 per consumer, per incident, or actual damages, whichever is higher, while the *California Invasion of Privacy Act*, statutory damages of US$ 5,000 per violation or treble actual damages may be awarded for unauthorized interception or recording, thereby limiting judicial discretion to determining amounts within a prescribed range or awarding higher proven damages. By contrast, the GDPR does not impose statutory caps; instead, it calls for a broad interpretation of compensable damage and requires remedies to remain "full and effective" in accordance with the principles of equivalence and effectiveness, leaving quantification largely to domestic courts.

While a purely open-ended European-style model may create unpredictability and inconsistency in Bangladesh's institutional context, a rigid fixed-sum model may also flatten the nuance required to assess emotional distress, dignitary harms, or aggravated violations in high-gravity cases. A hybrid approach may therefore be better suited for Bangladesh: the statute could establish indicative compensation ranges or baseline statutory damages for common categories of violations, while permitting higher awards where demonstrable actual harm, malicious conduct, systemic negligence, or severe non-economic injury can be established. For instance, the framework could prescribe indicative compensation ranges from BDT 10,000 to BDT 1,000,000 per consumer, per incident, depending on factors such as the sensitivity of the affected data, scale and duration of exposure, severity of resulting harm, vulnerability of affected individuals, intentionality or negligence of the controller or processor, and whether the violation involved children's or sensitive personal data, while permitting recovery of higher actual damages where the loss is specifically quantifiable. At the same time, the framework should expressly incorporate the principles of "full and effective" compensation and proportionality, while ensuring predictability, accessibility, and consistency within the Bangladeshi legal system.

Reintroduce accountability and sanctions framework for government agencies, statutory bodies, autonomous institutions, and their personnel. The statute should expressly provide that public-sector entities are subject to the same baseline data protection obligations, enforcement powers, corrective measures, civil penalties, and administrative sanctions applicable to private-sector actors, subject only to narrowly tailored and clearly defined exemptions grounded in necessity and proportionality. This framework should operate in parallel with existing legal safeguards — including anti-corruption laws, public service rules, criminal procedure code, and other administrative and criminal accountability mechanisms — which already provide for disciplinary proceedings and sanctions where misconduct is intentional, reckless, negligent, or repeated. Read together with the recommended safeguards relating to exemptions under section 24, such reforms would help ensure that public-sector data processing remains lawful, transparent, proportionate, and institutionally accountable, rather than effectively insulated from oversight or consequence.

To operationalize accountability, the law should further require mandatory logging and audit trails for access to sensitive government-held databases, periodic independent audits of public-sector data systems, internal authorization protocols for access to sensitive personal data, mandatory breach reporting obligations for government agencies, and publication of aggregate transparency reports concerning data requests, breaches, and enforcement actions. The statute should also expressly empower the NDMA to impose corrective measures such as mandatory audits, compliance orders, remediation directives, suspension of unlawful processing activities, and administrative penalties for unauthorized access, unlawful disclosure, negligent handling, or misuse of personal data by public authorities or their personnel.

2. National Data Management Act, 2026

The *National Data Management Act, 2026* establishes an expansive state-led digital governance framework centered around the NDMA, the NRDEX, and integrated digital public infrastructure systems. While intended to improve interoperability, administrative coordination, and digital service delivery, the framework raises significant concerns regarding institutional independence, concentration of data power, cybersecurity governance, and safeguards against misuse. In particular, the NDMA is formally described as an "independent" authority, yet its governance, appointment, funding, and oversight structures remain overwhelmingly executive-centric, raising concerns regarding its ability to function as an impartial regulator overseeing both state and private-sector actors. These concerns are amplified by the broad exemptions granted to state authorities under section 24 of the *Personal Data Protection Act, 2026*.

Additionally, the statute establishes a highly centralized interoperability and database integration architecture through mandatory integration of foundational citizen databases into the NRDEX framework, coupled with broad executive authority to classify and restrict exchange of "nationally important / sensitive data." Although interoperability may improve public service delivery, the cumulative framework creates risks of surveillance expansion, function creep, secondary use of personal data, cybersecurity vulnerabilities, and excessive concentration of sensitive citizen data within centralized state-linked systems. Furthermore, many core cybersecurity obligations — including incident response, penetration testing, encryption standards, vulnerability disclosure, and independent security auditing — remain underdeveloped or delegated to future regulations. Accordingly, we recommend narrowing broad executive powers, strengthening the institutional independence of the NDMA, prioritizing decentralized and privacy-preserving interoperability models, deleting or substantially reforming section 31, and introducing stronger cybersecurity, transparency, oversight, and human rights safeguards throughout the framework.

INSTITUTIONAL INDEPENDENCE

Sections 5, 8, 9, 12, 13, 15, 20, 21, 25, 26, 27, 35, 36, 38, 40 — Institutional design and independence of NDMA

ASSESSMENT

Although the statute formally declares NDMA to be "independent" under section 27, the institutional design raises substantial questions regarding the extent to which it can realistically function as an operationally, structurally, or politically independent regulator, particularly in matters involving government agencies, politically sensitive data processing, or national security-related exemptions.
From a governance structure perspective, both the NDMPB and the NDMA remain overwhelmingly executive-centric. For instance, the NDMPB is composed of seventeen ministers, parliamentarians, senior executive officials, and government appointees, and seven government-nominated civil society and subject-matter experts. While high-level national policy coordination bodies may be steered by the executive branch to facilitate inter-ministerial coordination, strategic direction, and implementation of national policy priorities, the same rationale cannot automatically be extended to a regulatory, oversight, enforcement, and adjudicatory authority such as the NDMA. Nevertheless, the institutional design of the NDMA itself remains

significantly executive-influenced. Appointments to the NDMA and its specialized wings are made by the government based on recommendations from a selection and review committee, itself dominated by senior executive officials and government nominees, without meaningful institutional safeguards to ensure genuine independence, pluralistic representation, or insulation from executive influence. This institutional independence is further complicated by financial and administrative dependence on the executive, with a substantial portion of the NDMA's fund being reliant on government grants and loans, and the Cabinet Division responsible for overall coordination and oversight of the agency. The government also retains significant influence over terms and conditions of service, appointments to key administrative positions, organizational structures, and financial arrangements, without independent parliamentary oversight. Collectively, these features create a model that more closely resembles an executive-affiliated regulatory body rather than a fully independent supervisory authority insulated from governmental influence.

This is particularly significant because the NDMA is simultaneously entrusted with regulatory, oversight, adjudicatory, enforcement, and policy-making functions over both public- and private-sector data processing. Absent stronger safeguards, there is a risk — or at minimum a reasonable perception — of selective enforcement, regulatory deference toward state actors, and politicized decision-making. When read with the broad exemptions conferred to state authorities in section 24 of the *Personal Data Protection Act, 2026*, this may result in the NDMA functioning more robustly as a regulator of private-sector entities, while exercising comparatively limited scrutiny over public-sector processing activities, particularly where national security, law enforcement, or politically sensitive interests are implicated. The concern, therefore, is not whether the statute formally labels the NDMA as "independent," but whether the cumulative institutional design provides sufficient structural autonomy and accountability safeguards to enable impartial and credible regulation of both private- and public-sector actors alike.

RECOMMENDATIONS

Amend provisions to ensure functional, operational, financial, and administration independence of NDMA.

Strengthen the institutional, operational, and financial independence of the NDMA. The statute should introduce stronger guarantees relating to appointment procedures, tenure security, removal protections, budgetary autonomy, and institutional insulation from executive direction to ensure that the NDMA can function as an impartial regulator overseeing both public- and private-sector actors. Particularly, appointments to the NDMA should be made through a more transparent and pluralistic process involving parliamentary scrutiny or confirmation, independent nomination procedures, and broader representation from opposition parties, civil society, academia, technical experts, and the legal profession, rather than remaining predominantly executive-controlled. Likewise, removal of members should also be limited to clearly defined statutory grounds and subject to procedural safeguards to prevent arbitrary executive interference. Moreover, the statute should further provide for greater financial and administrative autonomy by ensuring independent budgetary allocations approved through parliamentary processes, rather than substantial reliance on executive-controlled grants and administrative arrangements. Additionally, the law should also expressly clarify that the NDMA possesses equal authority to investigate, audit, issue directives against, and sanction government agencies, statutory bodies, and public officials, subject only to narrowly tailored exemptions grounded in legality, necessity, and proportionality. Such safeguards would help ensure that the NDMA functions as a genuinely independent supervisory authority rather than an executive-affiliated administrative body, thereby strengthening public trust, regulatory credibility, and the impartial enforcement of data protection obligations across both the public and private sectors.

Comparable frameworks expressly embed supervisory independence in the statute. For instance, South Africa's *Protection of Personal Information Act, 2013* establishes an independent regulatory body subject only to the

domestic constitution and the applicable laws, expressly requiring it to act without fear, favour, or prejudice and making it accountable to the national assembly rather than directly to the executive; meanwhile, the United Kingdom's *Data Protection Act 2018*, the regulator is required to exercise data protection functions with complete independence, while institutional arrangements provide for reporting obligations to the parliament, creating accountability mechanisms outside direct ministerial control.

An analogous example within the Bangladeshi context is the Anti-Corruption Commission, constituted under the *Anti-Corruption Commission Act, 2004*, which incorporates comparatively stronger structural safeguards for institutional independence: appointments are recommended by a selection committee comprising two judges of the Supreme Court of Bangladesh, two other constitutional bodies, and a retired cabinet secretary; it also enjoys comparatively greater financial and operational autonomy and is accountable to the president and the parliament, rather than functioning solely under direct executive supervision.

CROSS-BORDER DATA TRANSFER, DATABASE INTEGRATION AND CENTRALIZATION

Sections 30(6), 31, 32 — Centralized data-governance framework, compulsory localization of sensitive foundational databases, restrictions on nationally important and sensitive data

ASSESSMENT

The statute establishes an expansive interoperability and centralized data-governance framework through mandatory database integration, national data exchange infrastructure, and executive authority over certain categories of information. While these provisions may facilitate administrative efficiency and coordinated public service delivery, they also raise concerns regarding concentration of data power, cybersecurity resilience, institutional accountability, and the potential expansion of state surveillance capacities. Specifically:

(i) A mandatory interoperability and database integration framework is introduced in sections 30(6) and 32, requiring an undefined class of entities to integrate databases with the NRDEX, while also empowering the NDMA to require compulsory storage of such databases within national data centers if deemed expedient. Particularly, the framework expressly contemplates integration of highly sensitive foundational databases, including national identity records, passport databases, taxpayer information, address databases, birth registration records, and driving licence databases. On its face, this reflects a state-led effort to improve interoperability, administrative coordination, and digital service delivery through integrated digital public infrastructure.

However, the framework raises concerns regarding centralization, concentration of data power, cybersecurity resilience, and function creep. The aggregation and interoperability of multiple identity-linked state databases substantially increases systemic risk in the event of cyber compromise, insider misuse, unauthorized access, or unlawful secondary use. Moreover, the statute provides comparatively limited safeguards relating to compartmentalization, decentralized or federated architectures, strict purpose limitation enforcement, access separation, granular authorization controls, or restrictions on cross-context repurposing of integrated datasets. In practice, such large-scale interoperability systems may enable creation of highly granular and longitudinal citizen profiles

across multiple sectors of public life, particularly when combined with future AI-enabled governance systems and centralized data analytics capacities.

(ii) A broad category of "nationally important / sensitive data" is defined in section 31 as including information relating to sovereignty, territorial integrity, public safety, border security, constitutional emergencies, and information declared by the government as important or sensitive. The government is authorized to make rules and impose restrictions on the management, exchange, and sharing of such data. While differentiated protections for certain categories of strategically sensitive information are not uncommon in digital governance or cybersecurity frameworks, the provision is drafted in exceptionally broad and open-ended terms. Concepts such as "public safety" and "public order" remain statutorily undefined and jurisprudentially underdeveloped, making them susceptible to expansive interpretation, while broad discretion is afforded to the government to classify any other information under this provision. It also lacks meaningful procedural safeguards, including objective designation criteria, independent review mechanisms, mandatory public consultation. periodic reassessment requirements, or avenues for challenge and redress. As a result, the framework creates risks that restrictions on data exchange and classification powers may evolve beyond narrowly tailored cybersecurity or national security objectives into broader mechanisms for controlling information flows.

Read together, these provisions establish a highly centralized interoperability and data governance architecture combining mandatory integration of foundational citizen databases, broad executive authority over sensitive data classification and exchange, and expansive institutional powers within the NDMA ecosystem. Without robust procedural safeguards and institutional accountability mechanisms, the cumulative framework creates significant risks relating to concentration of state data power, cybersecurity vulnerabilities, and surveillance expansion, particularly in Bangladesh's context of evolving cybersecurity governance capacity, broad executive dominance, and recurring concerns regarding unauthorized access and disclosure of government-held data. The absence of stronger safeguards relating to decentralization, independent oversight, purpose limitation, access controls, institutional independence, judicial authorization, and human rights protections risks enabling disproportionate state access to interoperable citizen data systems and secondary use of personal information beyond the context in which it was originally collected. From a rights perspective, this may directly implicate privacy, informational self-determination, freedom of expression, freedom of association, anonymity, and democratic accountability.

RECOMMENDATIONS

Amend the interoperability and centralized database governance provisions, and delete section 31.
Amend the interoperability and centralized database governance framework to incorporate clearer statutory safeguards, institutional limitations, and independent oversight mechanisms. The statute should define with greater precision the categories of entities subject to mandatory database integration under sections 30(6) and 32, and should limit compulsory integration and centralized storage requirements to circumstances that are demonstrably necessary, proportionate, and supported by clearly articulated public-interest objectives. The law should also expressly prioritize decentralized or federated interoperability models where feasible, rather than defaulting to centralized storage architectures, and require enforceable safeguards relating to compartmentalization, purpose limitation, granular role-based access controls, data segregation, independent authorization mechanisms, immutable audit logging, and restrictions on secondary use or cross-context repurposing of integrated datasets.
Delete section 31 in its current form. While protection of genuinely sensitive state or national-security-related

information may be addressed through narrowly tailored sector-specific laws and cybersecurity frameworks, section 31 is drafted in exceptionally broad, open-ended, and discretionary terms that are incompatible with principles of legal certainty, necessity, and proportionality. In particular, undefined concepts such as "public safety" and "public order," coupled with the government's unrestricted authority to designate additional categories of "nationally important / sensitive data," confer excessively broad executive discretion without meaningful statutory limits, procedural safeguards, independent oversight, or judicial controls. Together with the broader interoperability and centralized data-governance architecture established elsewhere in the statute, the provision risks enabling opaque restrictions on information exchange, excessive concentration of state data power, surveillance expansion, and secondary use of citizens' data beyond the purposes for which such data were originally collected. If retention of such a framework is considered necessary, it should instead be enacted through a substantially narrower and separately legislated regime containing precise definitions, objective designation criteria, parliamentary oversight, independent review mechanisms, mandatory transparency obligations, and strict human rights safeguards.

DIGITAL PUBLIC INFRASTRUCTURE AND CYBERSECURITY

Sections 2(12), 2(13), 2(16), 23, 30, 33, 47, 48 — Digital public infrastructure, cybersecurity, interoperability, rule-making powers

ASSESSMENT

Although the statute does contain provisions relating to security, interoperability and protection of digital public infrastructure (like NRDEX), incorporating concepts such as zero-trust architecture, privacy-preserving principles, auditability, minimization, and interoperability, many of these issues remain underdeveloped, with substantial reliance placed on the NDMA and the government to formulate future rules, standards, certifications, and technical requirements on data governance and cybersecurity. It also leaves many core cybersecurity obligations — such as incident response, penetration testing, encryption standards, vulnerability disclosure, cyber resilience requirements, independent security audits, certification, authentication, and third-party vendor risk management — largely undefined or delegated to future regulations and directives.

At the same time, the framework remains comparatively underdeveloped in relation to operational cybersecurity governance, institutional accountability, and regulatory independence. It centralizes extensive interoperability and data exchange powers through digital public infrastructure without correspondingly strong safeguards, including decentralization, compartmentalization, insider-threat mitigation, purpose limitation, granular access controls, independent authorization mechanisms, data segregation, or limitations on function creep. As a result, in practice, this may create heightened systemic risks in the event of compromise, misuse, or unauthorized access, particularly in Bangladesh's context of evolving cybersecurity governance capacity and recurring concerns regarding unauthorized access and disclosure of government-held data. More broadly, the concentration of policy-making, infrastructure management, certification, standard-setting, adjudicatory, and enforcement functions within the same institutional ecosystem of the NDMA — combined with broad interoperability powers and extensive state-linked data integration — without sufficient procedural safeguards, raises legitimate concerns regarding independent oversight, accountability, surveillance expansion, and secondary use of citizens' data beyond originally stated purposes. From a human rights perspective, such risks may directly affect the rights to privacy, freedom of expression, freedom of association, informational self-determination, and anonymity, particularly where interoperable state-linked databases

enable large-scale profiling, tracking, monitoring, or repurposing of personal data beyond the original context in which it was collected, especially given the broad exemptions granted to government agencies and public authorities under section 24 of the *Personal Data Protection Act, 2026*.

RECOMMENDATIONS

Introduce rules to enhance safeguards for digital public infrastructure.

Introduce secondary legislations to strengthen the cybersecurity and governance framework for digital public infrastructure. The statute should move beyond broad architectural principles and formulate secondary legislations to expressly incorporate [correct?: procedural safeguards], like baseline cybersecurity obligations relating to incident response, encryption standards, coordinated vulnerability disclosure, penetration testing, cyber resilience planning, independent security audits, certification standards, third-party vendor management, and mandatory breach containment and recovery procedures. The law should also require privacy-by-design and security-by-design principles to be operationalized through enforceable obligations relating to data minimization, compartmentalization, decentralized or federated architectures where feasible, granular role-based access controls, purpose limitation enforcement, immutable audit trails, periodic access reviews, and strict logging requirements for access to sensitive government-held databases.

Additionally, the framework should introduce stronger institutional safeguards to prevent excessive concentration of power within the NDMA ecosystem. This could be achieved, for instance, by functionally and institutionally separating infrastructure management, standard-setting, certification, adjudication, and enforcement, subjecting them to stronger independent oversight and externally verifiable review mechanisms. The law should also require periodic independent cybersecurity assessments of digital public infrastructure systems, mandatory public reporting of aggregate cybersecurity incidents and audit findings, parliamentary oversight of large-scale interoperability systems, and human rights impact assessments prior to deployment of high-risk interoperable or AI-enabled public-sector systems.

3. Cyber Protection Act, 2026

The *Cyber Protection Act, 2026* largely reproduces many of the structural features, policy choices, and legal deficiencies of its predecessors and should therefore be substantially amended, as it remains inadequate for addressing contemporary online safety, content governance, and broader cybercrime challenges. It continues to reflect systemic legal, institutional, and enforcement deficiencies that have historically undermined constitutional rights and effective governance. Its overbroad and vague criminal provisions, particularly on speech, lack clear standards of harm, intent, and proportionality, leading to risks of arbitrary enforcement, over-criminalization, and chilling effects on free expression. Moreover, its notice-and-action framework is inadequate, as it relies on executive-driven takedown powers without adequate procedural safeguards, independent oversight, transparency requirements, or effective redress mechanisms, and does not impose clear, risk-based obligations on platforms to address systemic harms or ensure platform accountability. Importantly, the statute also removes, in its entirety, the safe-harbour protections that existed under earlier laws, thereby potentially exposing intermediaries and other platform operators to liability for third-party content without clear knowledge-based thresholds or due-diligence standards, which may incentivize over-removal of content and private censorship, further exacerbating chilling effects on lawful expression and access to information.

At the same time, the statute establishes a highly centralized institutional framework dominated by executive actors with limited independence, oversight, or accountability, while conferring expansive investigative, surveillance, and privacy-intrusive powers on LEAs without adequate procedural safeguards, judicial authorization requirements, or meaningful oversight mechanisms. Overall, these structural flaws — combined with jurisdictional overreach, deviations in enforcement from statutory protections, duplication and conflation of offenses, disproportionate penalties, weak implementation mechanisms, and inadequate safeguards for privacy, due process, and freedom of expression — render the statute substantially misaligned with principles of legality, legal certainty, due process, proportionality, and international human rights standards, thereby warranting substantial amendment or, alternatively, replacement through a more coherent and rights-respecting legislative framework.

If comprehensive reform is not undertaken, we recommend, in Part B, enacting a comprehensive online safety statute that addresses these shortcomings and establishes a unified framework for both content- and non-content-related harms, while ensuring meaningful accountability for state authorities through independent oversight, transparency, and procedural safeguards, and for platforms through risk-based obligations, duty-of-care standards, enforceable complaint and compliance mechanisms, and proportionate intermediary liability and safe-harbour protections.

SCOPE AND APPLICATION

Sections 3, 4 — Extraterritorial section authorizing prosecution of acts committed outside Bangladesh, even if inconsistent with other local and foreign law

ASSESSMENT

Application of the statute extraterritorially with an overriding effect raises concerns regarding jurisdictional overreach, conflicts of law principles, violations of sovereignty and non-interference principles, and tensions with international law and diplomatic relations. This approach also creates legal uncertainty and

enforcement challenges, potentially undermining the country's credibility as a law-abiding member of the global community and fostering distrust toward its legal system.

Here, section 4(1) reflects a nationality-based assertion of jurisdiction that requires clear procedural and substantive safeguards to avoid duplicative liability, conflicts with host state laws, and due process concerns when prosecuting acts committed abroad. Moreover, section 4(2) adopts a broad location-based approach tied to digital infrastructure in Bangladesh, but its low territorial threshold (based on mere use of systems located in Bangladesh) fails to adequately account for the inherently interconnected nature of the internet and digital infrastructure, while also risking overreach, legal uncertainty, and jurisdictional friction with other states where the conduct or actor is primarily situated. In both cases, establishing the jurisdictional threshold (whether through citizenship or a nexus to domestic digital infrastructure) poses significant evidentiary and logistical challenges that must be resolved prior to initiating proceedings for overseas conduct, thereby placing a substantial burden on investigators and courts to undertake careful legal assessment before framing offenses or pursuing cases.

RECOMMENDATIONS

Amend the provision to narrow the scope and application of extraterritorial jurisdiction.

Introduce clearly defined jurisdictional thresholds and nexus requirements, aligned with internationally accepted practices. As a criminal statute imposing punitive sanctions, its extraterritorial application should be limited to circumstances where there is a substantial, foreseeable, and direct nexus to Bangladesh. Jurisdiction should not arise solely because a digital system, server, or infrastructure component happens to be located within Bangladesh, nor solely on the basis of nationality. Instead, the statute should incorporate objective jurisdictional thresholds based on factors such as conduct occurring or producing substantial effects within Bangladesh, or conduct by overseas individuals or entities specifically targeting users, systems, or infrastructure within Bangladesh. Such an approach would reduce legal uncertainty, minimize conflicts with foreign laws, and better align the framework with principles of sovereignty, non-interference, due process, and international comity.

Comparative practice increasingly adopts more principled approaches. For example, European regulatory frameworks generally tie extraterritorial obligations to establishment, targeting of users, or substantial effects within the EU rather than mere technical connections to infrastructure. Specifically, the *Digital Services Act* states that the regulation will apply to services "offered to recipients of the service that have their place of establishment or are located in the [EU], irrespective of where the providers of those intermediary services have their place of establishment." Similarly, the United Kingdom's *Online Safety Act 2023* applies to services with a significant number of users, where the United Kingdom is a target market, or where there is a material risk of significant harm to users within the country. Even where legislation confers broad extraterritorial powers, courts have recognized practical and legal limits on their exercise. For instance, in *eSafety Commissioner v X Corp*, the Australian Federal Court declined to support a global removal order, observing that extending Australian law to regulate activities occurring wholly outside Australia and involving users with no connection to Australia would risk encroaching upon matters properly falling within the jurisdiction of other sovereign states. These developments reflect an emerging preference for clearly articulated nexus and substantial-effects approaches over expansive assertions of jurisdiction based solely on citizenship or incidental use of domestic infrastructure.

Bangladesh should replace the current approach with a more clearly defined nexus-based framework, such as requirement to consider, among other things, the location of affected persons, the intended target audience, the place where substantial harm occurred, the degree of connection to Bangladesh, the practical enforceability of any resulting orders, and the risk of conflict with applicable foreign laws.

INSTITUTIONAL STRUCTURE

Sections 5(3), 5(4), 7 — Authorities, functions and responsibilities of NCPA to be prescribed by rules, and organizational structure subject to government approval

Section 12 — Composed almost exclusively of state actors, and operating under direction of the prime minister, NCPC includes members of the DGFI, NSI, NTMC, BFIU, and Bangladesh Police.

ASSESSMENT

Despite its intended status as an independent statutory authority, the subordination of NCPA to a ministerial division — the Information and Communication Technology Division — raises concerns about its ability to protect citizens' rights and interests fairly, transparently, and independently, without undue government influence. Furthermore, leaving its authorities, functions, and responsibilities to be determined by rules risks creating a regulatory framework that is open to politicization. Autonomy and agency are necessary to fulfill statutory mandates and its overall legitimacy, and avoid instrumentalization by executive or political actors.

Composition of the NCPC, comprising two dozen members, raises concerns about the concentration of policy formulation and implementation authority within the executive branch, including eight law enforcement and intelligence agencies, with limited independent oversight and balanced representation.

Although members from the the National Human Rights Commission, judiciary, and two government-appointed private sector and human rights representatives are included, the absence of clear safeguards to ensure the impartiality and independence of their appointment and function risks reinforcing executive dominance rather than fostering inclusivity and diversity. The absence of independent experts, civil society representatives, legal scholars, and broader industry stakeholders significantly increases the risk of a narrow, security-centric approach, resulting in a governance model that is more likely to be politicized and reactive rather than proactive and rights-respecting in addressing cybersecurity challenges and online harms.

Taken together, these institutional design features indicate that the bodies lack meaningful independence and are not supported by adequate mechanisms for independent oversight, transparency, or accountability.

RECOMMENDATIONS

Reform the institutional architecture to ensure independence, accountability, and protection against undue executive influence.

Strengthen the institutional independence, governance, and accountability of cybersecurity and online safety bodies. The statute should expressly guarantee the institutional, operational, and financial independence of the NCPA by clearly defining its powers, functions, and responsibilities within the primary legislation rather than leaving core mandates, independence, and accountability mechanisms to subordinate rules, and subject the agency to appropriate multi-stakeholder parliamentary oversight. Appointment processes should likewise be transparent, merit-based, and subject to safeguards against undue executive influence.

Comparative practice increasingly favors independent digital, cybersecurity, communications, and online safety regulators, as reflected in the United Kingdom's Ofcom, Australia's eSafety Commissioner, and independent data protection and digital regulators across the EU.

Similarly, the composition of the NCPC should be rebalanced to reduce executive dominance and ensure broader representation from independent experts, academia, civil society, industry, technical communities, consumer representatives, and human rights institutions. While the Intelligence Agencies and LEAs should continue to play an important advisory and operational role, they should not dominate policy-making bodies responsible for developing national cybersecurity, digital governance, and online safety strategies. The statute should further establish clear accountability mechanisms, including parliamentary scrutiny, public consultation requirements, periodic reporting obligations, independent review processes, and judicial oversight, to ensure that both bodies remain transparent, effective, and accountable in the exercise of their powers.

SPEECH-RELATED OFFENSES

Online speech criminalized under the statute includes:

(A) section 25 — content created, obtained, or stored, including those generated or modified using AI, for the purposes of:
- ***a. sexual harassment***
- ***b. revenge porn***
- ***c. child sexual abuse material***
- ***d. sextortion***
- ***e. blackmail***

(B) section 26 — use and transmission of identity information, for the purposes of:
- ***a. religious disharmony***
- ***b. communal or ethnic hatred***

(C) sections 26 and 29 — aiding in the commission of offenses, and individual liability for corporate conducts

ASSESSMENT

Criminalization of these online speech is inadequate as the provisions are overbroad and insufficiently differentiated, lacking clear standards of harm, intent, and enforcement, thereby creating risks of arbitrary and disproportionate application, gaps in coverage of emerging harms, and failure to meet constitutional and international human rights requirements.

(A) While this provision recognizes and defines a wide array of technology-facilitated harms and abusive conduct, especially against women and children, and its inclusion of both actual publication or dissemination and threats to do so strengthens its overall scope, it aggregates distinct forms of harm under a single provision with a unified penalty regime without accounting for differences in severity and impact. As such, the provision remains overly broad and insufficiently differentiated, conflating distinct categories of harm and risking ambiguity in interpretation and enforcement. Specifically:

- Certain definitions cover some harm areas but do not fully address all relevant categories of technology-facilitated abuse. For instance, non-consensual intimate image abuse, deepfakes, and online grooming and child solicitation appear to be partially covered within existing definitions. However, embedding distinct harms within broader umbrella definitions rather than treating them as separate offenses, and conflating conduct-based offenses (e.g., harassment, coercion, grooming) with content-based offenses (e.g., CSAM or non-consensual pornography) without clear doctrinal separation, undermines conceptual clarity and proportional

enforcement. Absent clearer offense differentiation, offense gradation, or sentencing guidance, this structure places significant reliance on judicial discretion and may therefore result in inconsistent and potentially disproportionate penalties, with similar conduct attracting divergent outcomes across cases.

- Certain key definitions themselves remain either underinclusive or excessively broad and structurally incoherent. For instance, the definition of "revenge porn" is conceptually outdated and narrowly focused on dissemination; in fact, the expression itself is increasingly considered inadequate and misleading because such conduct is not always motivated by "revenge," nor is the material necessarily "pornographic." Moreover, the offence should not be conditioned on proving intent to cause harm, as this introduces a subjective intent threshold that may unnecessarily narrow liability and create evidentiary difficulties. It also potentially excludes other forms of image-based sexual abuse such as threats of dissemination, non-consensual recording, synthetic or AI-generated intimate imagery, voyeuristic capture, or commercial exploitation that would fall within more appropriate and preferable terms such as "non-consensual intimate imagery" or "non-consensual pornography." A more technologically neutral and internally structured formulation — such as the proposed definitions of "non-consensual pornography" in our recommendations to the definition section of the Pornography Control Act, 2012 above — would provide greater legal certainty, better reflect contemporary forms of online abuse and exploitation, improve conceptual clarity, and reduce risks of overbreadth, evidentiary uncertainty, and inconsistent interpretation.

- Certain behaviors (such as cyberstalking, doxxing, technology-facilitated surveillance, gender-based hate speech, targeted disinformation, sexualized harassment campaigns, and coordinated online abuse campaigns) are either not covered or insufficiently addressed. By comprehensively and prescriptively listing and defining certain harms while omitting others, the provision risks excluding emerging and equally harmful forms of technology-facilitated abuse from its scope.

- The harms listed in this provision are conditioned on having a "harmful or intimidating" effect, meaning that offenses such as sextortion, revenge porn, or child sexual abuse material are not treated as per se or strict liability offenses, but instead depend on a subjective assessment of harm or intimidation. This may raise evidentiary thresholds, create inconsistency in enforcement, weaken protection for victims, and open avenues for misuse or selective application against individuals, particularly in cases where harm is inherent but difficult to prove.

(B) This provision seeks to address online hate speech by criminalizing the publication or dissemination of content associated with religious, communal, or ethnic animosity that leads to violence, fear, or disorder, reflecting a legitimate state interest in maintaining public order. However, the provision is broadly framed and lacks clear definitional thresholds for key terms such as "hatred," "fear," or "disorder," creating risks of overbroad interpretation, subjectivity, and potential encroachment on lawful expression, particularly in politically or socially sensitive contexts. Moreover, framing the offense primarily through categories such as "religious," "communal," or "ethnic" hatred risks reinforcing and entrenching social, sectarian, and communal divisions by presuming that such incidents are necessarily rooted in identity-based hostility. In practice, episodes of violence or unrest that are characterized as religious or communal are often driven by a range of underlying factors, including political mobilization, local power struggles, economic grievances, personal disputes, criminal opportunism, or coordinated disinformation campaigns, with identity serving merely as a vehicle or pretext rather than the true motivating cause. Such formulations may therefore obscure the underlying drivers of harmful conduct while simultaneously amplifying identity-based narratives.

Further, since the publication or dissemination of such content is not an offense per se unless it results in violence, fear, or disorder, the provision introduces an additional burden to establish causation and intent. This requires authorities not only to characterize the speech as religious, communal, or ethnic in nature, but also to demonstrate a causal connection between the communication and the resulting harm, creating significant evidentiary complexity and increasing reliance on subjective assessments. This may lead to inconsistent application, heightened reliance on judicial discretion, and potentially disproportionate outcomes and misuse against individuals, thereby blunting the overall effectiveness of the law.

Across both sections 25 and 26, publication and dissemination have been criminalized, which is only effective in holding users liable if they are identifiable, meaning that there are likely to be enforcement challenges where users use pseudonyms or operate anonymously. However, the statute lacks clear enforcement mechanisms where users are not identifiable.

Moreover, comparable frameworks adopt a broader, more granular taxonomy of online harms, encompassing both user-based liability and systemic platform liability. With respect to user liability, these include non-consensual disclosure of intimate content, altered or synthetic (including non-sexual) images, violent material, age-inappropriate content exposure, doxxing, cyberflashing, coordinated inauthentic behavior and harassment, use of tracking technologies for monitoring or coercion, promotion or facilitation of serious self-harm and suicide, and sending false or unsolicited communications. Additionally, many frameworks recognize harms arising from systemic failures that attract platform liability — including algorithmic amplification of harmful content, lack of effective user reporting and redress mechanisms, failure to act on notices of harmful content, inadequate content moderation systems and safeguards, unsafe or manipulative design features, and failure to prevent misuse of platform functionalities (e.g., livestreaming, private messaging, or group features) — thereby reflecting systemic- and risk-based regulation and duty-of-care obligations on intermediary platforms, which are largely absent from the existing framework. As currently drafted, these provisions remain narrowly focused on specific user-level, content-based offenses, without incorporating a comprehensive or differentiated framework of harms or addressing platform-level responsibilities, thereby limiting their effectiveness in responding to the full spectrum of technology-facilitated harms.

(C) Across substantive speech-related provisions, only publication and dissemination have been criminalized, which limits enforcement against user-generated content platforms, as the platforms are generally not treated as publishers or transmitters but as intermediaries and content hosts. One of the avenues through which platforms can be held liable, albeit indirectly, is section 27 read with section 29, for aiding in the commission of an offense. However, a central challenge in establishing such secondary liability is that it remains conditional on identifying the primary offender, and then demonstrating that the platform had the necessary knowledge and/or intent to aid in the commission of the offense. Once that is established, under section 29, owners, senior management, and other employees and representatives associated with the platform can also be held liable, unless it is shown that they were either unaware of the offending content or that reasonable efforts were made to prevent the offense. These cumulative requirements set a demanding evidentiary standard, which may significantly constrain the ability to attribute liability to platforms in practice — and to this date, there are no successful cases of platform liability. However, no direct substantive provision exists to address system- or process-level failures, thereby limiting accountability for platform design, moderation, or governance shortcomings.

RECOMMENDATIONS

Amend the provisions to modernize the online harms framework through clearer offense definitions, differentiated categories of harm, platform accountability obligations, and stronger procedural safeguards.

Expand, differentiate, and modernize the taxonomy of online harms. The statute should move away from aggregating diverse forms of technology-facilitated harms under broad and overlapping provisions and instead adopt a more differentiated framework that clearly distinguishes between distinct categories of offenses. Currently, the framework does not capture the broad range of offenses committed online. Separate and clearly defined offenses should be established — through dedicated provisions where appropriate — for CSAM, non-consensual intimate imagery, deepfake and synthetic intimate imagery, sextortion, online grooming and child solicitation, cyberstalking, doxxing, technology-facilitated surveillance, cyberflashing, coordinated online harassment, gender-based online violence, and other serious forms of technology-facilitated abuse. Moreover, the statute should replace outdated and imprecise terminology with technologically neutral and clearly defined concepts. Particularly, terms such as "revenge porn" should be replaced with broader concepts such as "non-consensual intimate imagery" or "non-consensual pornography," expressly covering threats of dissemination, voyeuristic capture, synthetic or AI-generated content, non-consensual recording, and commercial exploitation. The framework should further distinguish between offenses based on severity, intent, harm, victim vulnerability, and aggravating factors, supported by clear statutory sentencing guidance to promote proportionality and consistency.

Comparative frameworks supporting this differentiated and well-defined approach include the EU *Digital Services Act* and the *Directive on combating violence against women and domestic violence*, the United Kingdom's Online Safety Act 2023, Singapore's *Online Safety (Relief and Accountability) Act 2025* and *Online Criminal Harms Act 2023*, Australia's *Online Safety Act 2021*, and New Zealand's *Harmful Digital Communications Act 2015*. Collectively, these frameworks move beyond broad and undifferentiated criminalization of online harms within a single provision and instead adopt more granular categories of harmful conduct, differentiated enforcement mechanisms, notice-and-action procedures, platform duties of care, transparency obligations, and enhanced protections for vulnerable groups.

Refocus online hate-speech provisions on demonstrable harms rather than identity-based causes. The statute should move away from criminalizing communications on the basis that they promote or disseminate "religious disharmony" or "communal or ethnic hatred," as such formulations are inherently subjective and risk obscuring the underlying drivers of harmful conduct while simultaneously reinforcing identity-based narratives and social divisions. Moreover, they require authorities and courts to establish the meaning and scope of inherently contested and insufficiently defined concepts such as "religious," "communal," "ethnic," "hatred," "fear," and "disorder," while also proving causation and, where applicable, intent. Instead, the provision should focus on clearly identifiable and demonstrable harmful effects, such as incitement to violence, incitement to discrimination, incitement to hostility, targeted intimidation, or other objectively ascertainable harms. Such an approach would better align with constitutional requirements of legal certainty, necessity, and proportionality, while still capturing harmful conduct motivated by religious, communal, ethnic, racial, political, or other forms of identity-based animus.

Comparative frameworks increasingly adopt effect-based formulations. For example, Singapore's *Online Safety (Relief and Accountability) Act 2025* defines "incitement of violence" as "the communication of online material that a reasonable person would conclude incites or is likely to incite one or more persons to use unlawful force or unlawful violence against any group in Singapore." Similarly, international human rights frameworks, including Article 20(2) of the ICCPR and the *Rabat Plan of Action*, focus on advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence, rather than on

vague or subjective notions of disharmony, fear, or disorder. Accordingly, any retained concepts such as "hatred," "fear," "hostility," or "disorder" should either be deleted or accompanied by clear statutory definitions and objective thresholds to reduce ambiguity, constrain discretion, and minimize risks of arbitrary, inconsistent, or politically motivated enforcement.

Clarify platform accountability and safe-harbor protections. The statute should establish a clear framework for direct platform accountability that distinguishes between content creators, users, hosts, intermediaries, and platform operators, as well as between different categories of platform operators. Current formulation of secondary liability should not be the sole mechanism for attributing intermediary liability. Instead, platforms should be subject to proportionate obligations calibrated to factors such as functionality, knowledge, control, technical capability, risk exposure, degree of control, and compliance with statutory duties of care. At the same time, safe-harbor protections should be preserved for intermediaries that act expeditiously upon receiving lawful notices and comply with prescribed notice-and-action procedures, risk-mitigation measures, and content-governance obligations. Absent such protections, the statute risks over-criminalizing intermediaries and platform operators for third-party conduct over which they may have limited visibility or control.

Comparative frameworks increasingly adopt such differentiated approaches. For example, the EU *Digital Services Act* maintains conditional liability exemptions for intermediary services while imposing due-diligence, notice-and-action, transparency, and systemic risk-mitigation obligations. Similarly, Australia's *Online Safety Act 2021* and the United Kingdom's *Online Safety Act 2023* does not treat platforms as publishers of all user-generated content, but instead imposes duties of care and risk-management obligations proportional to the nature, functionality, and size of the service. Singapore's *Online Safety (Relief and Accountability) Act 2025* and *Online Criminal Harms Act 2023* similarly impose targeted obligations on online services to address specified harms without imposing strict publisher liability for all user content. Bangladesh should adopt a similarly balanced framework that ensures meaningful platform accountability for systemic failures, repeated non-compliance, reckless disregard of statutory obligations, direct intermediary liability where appropriate, or deliberate facilitation of unlawful online harms.

Section 8 — Authority to remove or block content on specific grounds

ASSESSMENT

Although this provision purports to establish a framework for online content restrictions, it reflects a broad, executive-led takedown power without sufficient procedural clarity, judicial safeguards, or alignment with substantive offenses, raising risks for both overreach and under-enforcement. Specifically:

(i) The provision does not meet the requirements of an established notice-and-takedown regime. It only addresses government-initiated takedown procedures and does not provide an avenue for users to report harmful or illegal content. Moreover, there are no clear standards of care for platforms against which legal assessments are to be made, nor, once a takedown order is issued, are there procedural safeguards such as notice to affected parties, opportunity to contest, defined timelines for compliance, or appeals and other redress mechanisms. It also errs on the side of takedown (e.g., blocking or removal), rather than adopting a graduated set of measures (e.g., restriction, demotion, age-gating, removal, geo-blocking, or global blocking). Overall, the process is largely executive-driven, with limited clarity on how decisions are made, reviewed, or challenged.

(ii) The use of the term "request" to technology companies for content takedown is ambiguous and contradictory in this context, creating uncertainty as to whether it implies a non-binding recommendation

or carries the force of an enforceable directive, especially given there are no clear penalties for non-compliance.

(iii) There is no prior judicial authorization requirement for takedown orders nor any clear guidelines on how decisions can be challenged. Although subsection (4) introduces a requirement for ex post tribunal approval within three days, the initial removal or blocking can occur without prior judicial authorization. This raises concerns about overbroad executive discretion, particularly in the absence of clear criteria ensuring that restrictions meet constitutional grounds (e.g., national security, public order) and international human rights standards of legality, necessity, and proportionality. Rather, the tribunal's role appears reactive rather than substantive, and is not based on clearly articulated standards, potentially limiting meaningful oversight. Although the provision mandates restoration of content if such approval is not obtained within the prescribed timeline, it does not articulate how this requirement will be operationalized in practice, ensure that restoration occurs, or specify consequences for regulatory non-compliance.

(iv) There are internal inconsistencies and ambiguities in the allocation of powers. The authority to initiate takedown is diffused across the LEAs, BTRC, DG-NCPA, other agencies under the Information and Communication Technology Division, and even the tribunal, without a clear hierarchy or delineation of roles, creating a confusing and potentially overlapping enforcement architecture. This multiplicity of issuing authorities creates fragmentation and weakens accountability, making it difficult to trace responsibility for decisions and increasing the risk of arbitrary or inconsistent enforcement.

(v) There is a misalignment with the substantive provisions of the statute. While other sections criminalize a wide range of offenses (see above), this provision narrows its operational focus to select broad and undefined categories such as cyber security threats, public order concerns, communalism, and hate speech. This not only compounds ambiguity and risks inconsistent application, but, by not clearly linking takedown powers to the full spectrum of offenses, also risks limiting the availability of takedown measures to only certain types of content. This selective scope may result in uneven enforcement and gaps in addressing other forms of harmful or unlawful content.

(vi) The delegation of authority to prescribe rules without clear legislative guidelines risks regulatory overreach, creates legal uncertainty and enforcement inconsistencies, and may expand the scope of the law beyond legislative intent, particularly if such rules are developed without sufficient transparency or public input.

RECOMMENDATIONS

Amend the provision to establish a comprehensive notice-and-action framework.

Replace the broad and discretionary executive-led content-removal framework with a rights-respecting notice-and-action regime. This framework should clearly define the circumstances, procedures, authorities, and safeguards applicable to content restrictions. It should also establish accessible mechanisms enabling users, trusted flaggers, regulators, and LEAs to report unlawful content, while imposing corresponding obligations on platforms to assess and respond to lawful notices within prescribed timeframes. Any government-led content-removal function should be vested in a single nodal authority to avoid overlapping mandates, fragmentation, and inconsistent enforcement.

Any restriction on online content should be grounded in clearly defined statutory offenses and objective legal standards (rather than broad and undefined categories such as cyber security threats, public

order concerns, communalism, or hate speech), and should remain subject to the principles of legality, necessity, proportionality, transparency, and due process. Moreover, rather than relying exclusively on removal or blocking, the statute should provide for a graduated range of interventions, including labeling, warning notices, age-gating, visibility restrictions, demonetization, demotion, geo-blocking, temporary restriction, removal, and, only in exceptional circumstances, service-wide blocking. Significant content-restriction measures should be accompanied by procedural safeguards, including notice to affected parties, reasons for decisions, counter-notice procedures, appeal rights, independent review mechanisms, and restoration procedures where content is found to have been wrongfully restricted.

The statute should further clarify the legal nature and effect of takedown directives by replacing ambiguous terminology such as "request" with clearly defined categories of voluntary requests, lawful notices, emergency orders, and binding directives, each subject to distinct procedural requirements and legal consequences.

Except in narrowly defined emergency circumstances involving imminent threats to life, CSAM, terrorism-related content, or similarly serious harms, significant content-removal or blocking orders should be subject to prior judicial authorization or independent adjudicatory review. Where emergency powers are exercised, prompt ex post judicial review, transparency reporting, and clear restoration obligations should apply. The law should also expressly define the standards governing approval, review, restoration, and challenge of content-restriction decisions, including consequences for regulatory non-compliance.

Comparative frameworks have long adopted such approaches. For instance, the EU *Digital Services Act* establishes detailed notice-and-action procedures, transparency obligations, trusted flagger mechanisms, statement-of-reasons requirements, and user redress processes. Australia's *Online Safety Act 2021* combines notice-and-removal mechanisms with review and accountability safeguards, while Singapore's *Online Safety (Relief and Accountability) Act 2025* provides structured procedures governing content directions, review rights, and regulatory oversight. Similarly, India's *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021* combine intermediary due-diligence obligations, notice-based compliance mechanisms, and conditional safe-harbor protections. Bangladesh should adopt a similarly transparent, proportionate, and accountable framework that ensures a meaningful accountability mechanism for platforms.

Sections 25 and 26 — Criminal penalties for up to five years' imprisonment and BDT 20,000,000 fine

ASSESSMENT

A penalty regime imposing up to two years' imprisonment and BDT 10,000,000 fines (increasing to five years' imprisonment and BDT 20,000,000 fines for crimes committed against women and children) for a broad range of offenses without clearly differentiating between levels of culpability, harm, or intent appears disproportionate. Absent sentencing guidelines, a recommendation system, or a central database of decided cases, judges are left with broad discretion, which undermines consistency in sentencing, and may result in an arbitrary, disproportionate, and fragmented penalty regime, systemic biases and inequalities in sentencing, and failure to achieve broader social goals such as deterrence and rehabilitation — thereby infringing equal protection and legal certainty principles, as well as the right to a fair trial, and undermining public confidence in the judiciary and the rule of law. Especially given the unevenness of sentencing across other penal statutes, the higher penalties under this law appear to run counter to the rights to free speech, equality before the law, and due process guarantees enshrined in constitutional and international human

rights frameworks.

Further, the law prescribes the same penalties for aiding or abetting as for the principal offense, without differentiating degrees of participation or culpability, which risks compounding disproportionality and inconsistent application, especially in relation to platforms; at the same time, the absence of any direct substantive provision addressing system- or process-level failures by platforms limits the ability to impose sanctions for platform design, moderation, or governance shortcomings.

RECOMMENDATIONS

Amend the provisions to establish a more structured, proportionate, and differentiated penalty framework for online harms.

Introduce a more proportionate, differentiated, and structured penalty framework. The statute should calibrate penalties according to the nature of the offense, degree of harm, intent of the offender, vulnerability of the victim, and level of participation in the offending conduct, rather than imposing broadly similar penalties across a diverse range of offenses. It should therefore establish differentiated sentencing bands, offense-specific penalty frameworks, and clear aggravating and mitigating factors, while requiring the development of sentencing guidelines, judicial bench books, sentencing databases, or comparable mechanisms to promote consistency and legal certainty. The framework should also ensure that penalties remain broadly aligned with comparable offenses under other statutes and reflect the relative seriousness of the conduct involved. Furthermore, it should distinguish between principal offenders, aiders and abettors, facilitators, negligent actors, reckless actors, and intentional offenders, rather than automatically imposing identical penalties irrespective of culpability. Digital platforms and intermediaries should be held liable for systemic failures, repeated non-compliance, reckless disregard of statutory obligations, or deliberate facilitation of unlawful conduct, complemented by proportionate civil, administrative, and regulatory sanctions for platform-level design, moderation, governance, or compliance failures, while reserving criminal penalties for the most serious, harmful, and intentional forms of misconduct.

Sections 46, 31(3), 31(4) — Cognizability and non-bailability of offenses

ASSESSMENT

Offenses under Section 25 are cognizable, while those under Section 26 are non-cognizable. Cognizability allows law enforcement to arrest without a warrant and initiate investigations without prior judicial approval, whereas non-cognizability requires a warrant for arrest. Both offenses are classified as bailable, meaning bail should be granted as a matter of right. Moreover, subsections (3) and (4) of section 31 require that, in cases filed under these provisions, evidence, including the complainant's testimony, be presented before a magistrate within 24 hours, who must determine whether sufficient grounds exist to proceed with an investigation or dismiss the complaint and order the release of the detained person.

However, despite this classification and safeguards, an initial review of publicly available media reports suggests that around two dozen individuals have been arrested and some were held in custody for speech-related offenses between September 16, 2024 and May 2, 2026 under this statute and its predecessor, the Cyber Protection Ordinance, 2025. Such practice appears inconsistent with the statutory framework, and the use of arrest and pretrial detention in these

cases risks undermining constitutional protections, including the presumption of innocence, protection against arbitrary detention, and the right to a fair trial. It also runs counter to the policy rationale behind these classifications and safeguards, which is to reserve coercive powers for serious and high-priority offenses, while ensuring that cases lacking merit are dismissed and less serious offenses are addressed through proportionate and non-custodial measures.

RECOMMENDATIONS

Amend the provisions to make non-serious speech-related offenses non-congizable and bailable.

Strengthen safeguards against arrest and pretrial detention for speech-related offenses. The statute should clarify that arrest, detention, and other coercive investigative powers are exceptional measures reserved for serious offenses and clearly defined circumstances involving necessity, flight risk, evidence tampering, witness intimidation, or serious threats to public safety, rather than routine responses to speech-related offenses. LEAs should be required to comply strictly with statutory requirements relating to cognizability, bailability, and prompt judicial scrutiny, while courts should prioritize non-custodial measures wherever appropriate. Where custodial measures are necessary in exceptional cases, the law should provide additional safeguards against arbitrary arrest and prolonged pretrial detention, including enhanced judicial oversight, periodic review of detention, reporting obligations, and effective remedies for non-compliance. Such measures would better ensure consistency with the presumption of innocence, protection against arbitrary detention, due process guarantees, and the overall objective of addressing less serious offenses through proportionate and rights-respecting enforcement mechanisms.

Sections 28, 40 — Penalties for filing false complaints and cases, and cases only to be filed by aggrieved person

ASSESSMENT

Although this provision seeks to deter false and malicious complaints by criminalizing the filing of baseless cases, its practical effectiveness is constrained by inadequate procedural safeguards and inconsistent compliance. For instance, section 40 allows only complaints filed by a person directly aggrieved, an authorized representative, or a member of law enforcement; however, publicly reported cases indicate that complaints filed by political activists have nonetheless been registered and acted upon, including two arrests in Panchagarh in April 2026, in relation to content involving notable political figures from the ruling party, suggesting deviations from statutory requirements in practice. This enables proxy, retaliatory, or politically motivated complaints to proceed without adherence to procedural safeguards.

Moreover, the absence of clear evidentiary or procedural thresholds at the stage of filing or investigation lowers the bar for initiating criminal proceedings and increases the likelihood that cases lacking substantive merit proceed through the system, with many ultimately dismissed only after prolonged trial processes. Given the cognizable nature of several underlying offenses and the practice of prompt enforcement action, such complaints can trigger swift arrests, pretrial detention, legal uncertainty, financial burden, and reputational harm, even where evidentiary thresholds for criminal liability are not met. Its effectiveness remains highly contingent on judicial discretion, and the absence of clear standards for what constitutes a "lawful" or "just" complaint limits its deterrent value, thereby failing to prevent the statute from being used as a tool of harassment.

RECOMMENDATIONS

Amend the provisions to ensure

Strengthen safeguards against frivolous, proxy, and politically motivated complaints. The statute should reinforce the requirement that complaints be initiated only by genuinely aggrieved persons, authorized representatives, or clearly designated public authorities acting within their statutory mandate, while introducing clearer evidentiary and procedural thresholds before criminal investigations, arrests, or other coercive measures may be initiated. Courts and investigating authorities should be required to conduct an early assessment of standing, evidence, and legal sufficiency before proceeding with cases, particularly in relation to speech-related offenses. The law should further clarify the standards for determining malicious, vexatious, or bad-faith complaints and provide effective sanctions, compensation mechanisms, or other remedies against abuse of process. Such reforms would reduce opportunities for proxy litigation, political misuse, harassment, and retaliatory complaints, while ensuring that legitimate victims retain meaningful access to legal remedies and that criminal proceedings are reserved for cases supported by credible evidence and genuine public interest.

NON-SPEECH OFFENSES

Other actions criminalized under the statute includes:

(A) section 17 — accessing critical information infrastructure illegally

(B) section 18 — accessing computer, digital device, computer system or networks illegally

(C) section 19 — offenses against computers and computer systems and networks, including phishing, malware, and cyber ransom

(D) section 20 — online gambling

(E) section 21 — cyber forgery

(F) section 23 — cyber terrorism

(G) section 24 — e-transaction without legal authority

ASSESSMENT

Cyber offenses criminalized in this statute are inadequate for the following reasons.

(A) Broad wording of sections 17 and 18 — prohibiting intentional illegal access, alteration, or corruption of critical information infrastructure, computer systems and networks, databases, and digital devices, or attempts or abetments to do so — fails to outline the degree of "harm" or "damage" required for an offense. Without clear definitions and limitations, and in the absence of judicial precedent, there is a risk that such vagueness may lead to overly broad interpretation, and the provision could be used to target individuals or organizations. A blanket criminalization of "illegal access" and its abetment or attempt, regardless of the context or intent, and without distinguishing between malicious actors and those seeking to improve security (e.g., cybersecurity researchers), may stifle innovation and discourage proactive efforts to identify and mitigate vulnerabilities, thereby undermining broader cybersecurity goals. Under its current formulation, for instance, the cybersecurity researcher Viktor Markopoulos identifying vulnerabilities in the government website resulting in data breach could be exposed to criminal liability under this provision. Such ambiguities undermine the principle of legality, which mandates that laws must be sufficiently clear to allow individuals to understand what behavior is prohibited. Moreover, the lack of specificity could hinder effective security measures, as robust cybersecurity frameworks depend on clearly defined thresholds of harm and nuanced differentiation between types of conduct and risk.

(B) See the comments in (A) above.

(C) Bundling multiple distinct offenses, involving different levels of harm, intent, and complexity, into a single provision without adequately differentiating between their severity or intent is

contrary to essential principles in constitutional law such as legal certainty and proportionality. For instance, the act of "unauthorized collection of any data, database, information, or excerpts thereof" from a computer system appears to be treated with the same gravity as "intentionally introducing any type of infectious, malware, or harmful software" or "intentionally sending unsolicited electronic phishing mail or ransomware mail," despite the vastly different potential harms these actions can cause. Uniform treatment of fundamentally distinct offenses attracts disproportionate penalties and arbitrary enforcement, contrary to due process and fair trial principles, leading to over-criminalization. It risks stifling innovation and good-faith activities — such as ethical hacking, penetration testing, and cybersecurity research — in the digital space. Ultimately, this weakens the overall security posture of the digital ecosystem.

(D) While this provision criminalizes gambling in cyberspace through a broad prohibition on creation, operation, participation, assistance, and promotion of gambling-related activities, its broad and undifferentiated scope, combined with the absence of definitional clarity and gradation of liability, raises two major concerns.

- The provision does not define "gambling," creating ambiguity in scope. Absent clear statutory definition distinguishing games of chance from games of skill, or clarifying elements such as wagering, consideration, and prize, the provision risks overbreadth; this could bring within its ambit a wide range of activities, such as online gaming, fantasy sports, esports competitions, or promotional contests, that may not traditionally constitute gambling under comparative legal standards. While the courts in Jafar Ullah vs Bangladesh and Mohammad Samiul Huq vs Bangladesh have attempted to clarify remit of gambling-related provisions in earlier laws, these judicial interpretations are limited in scope and do not provide comprehensive or prospective guidance, thereby leaving continued uncertainty in application and enforcement. The lack of definitional clarity may therefore lead to inconsistent interpretation and enforcement, and potential over-criminalization of legitimate digital economic activity.

- It also aggregates distinct roles and levels of involvement, including operators, participants, advertisers, and those who "assist or encourage," under a single offense and penalty framework, without differentiating degrees of culpability, intent, or benefit. This undifferentiated liability structure risks disproportionate penalties, particularly where passive actors (e.g., participants) and peripheral actors (e.g., advertisers or intermediaries) are treated on par with operators or organizers. This creates a low threshold for liability that may capture incidental or indirect conduct, raising concerns about potential spillover into lawful expression or commercial speech, particularly in the absence of clear intent or knowledge requirements. Moreover, this undifferentiated approach extends to the penalty regime, imposing up to two years' imprisonment and substantial fines extending up to BDT 10,000,000, which appears to apply uniformly across all forms of conduct covered under the provision, without graduation based on scale, harm, or intent, thereby raising concerns about proportionality.

(E) This provision criminalizes "cyberspace forgery" through a broad formulation, which raises concerns about overbreadth, duplication, and lack of doctrinal clarity. While parts of the definition align with traditional notions of forgery, it extends to a wide range of activities — including digital document creation, illicit cross-border transactions, SIM misuse, mobile banking operations, cryptocurrency transactions, and even gambling-related conduct — many of which overlap with other provisions of the statute, creating risks of duplication, multiplicity of charges for the same underlying conduct, and exposure to differing penalty regimes for similar acts. For instance, the immediately subsequent provision on "cyberspace fraud" (defined as manipulation of digital information to

reduce its value or usefulness, obtain financial or other benefits, or cause harm), along with the preceding provision on gambling, covers several of the same activities, thereby blurring doctrinal boundaries between forgery, fraud, and other cyber offenses. This expansive and overlapping scope risks conflating distinct legal categories and lowering the threshold for criminal liability. Coupled with a uniform and relatively severe penalty framework that does not differentiate based on harm, scale, or sophistication, the provision raises concerns about proportionality, legal certainty, and potential over-criminalization.

(F) This provision criminalizes "cyber terrorism" by covering a wide range of activities affecting national security, critical infrastructure, and public order; however, its broad and composite drafting raises concerns of overbreadth, conceptual conflation, and potential misuse. While certain elements (e.g., attacks on critical infrastructure or actions causing death or serious injury) align with internationally recognized thresholds for cyber terrorism, the inclusion of vaguely defined acts — such as accessing computer systems or data that "may be used" against state interests, affecting friendly relations with a foreign state, or benefiting a foreign state — without adequate definitional clarity, safeguards, or exemptions introduces subjective and expansive criteria that risk capturing conduct beyond genuine terrorism-related activity. It may have a chilling effect on freedom of expression and press, particularly where journalistic investigation, research, or reporting on matters of public interest, or even social media posts criticizing the government or foreign state, could be construed as falling within its scope. Aggregation of distinct forms of conduct under a single offense, without clearly distinguishing between levels of harm, intent, or impact, and its overlap with other sections creates risks of duplication and multiplicity of charges for the same conduct while blurring doctrinal boundaries between cybercrime and terrorism. Coupled with a uniform and severe penalty framework, imposing up to ten years' imprisonment and fines extending up to BDT 10,000,000, without clear gradation based on harm or intent, the provision raises concerns about proportionality, legal certainty, and the risk of arbitrary or inconsistent enforcement.

(G) While it is necessary to have codes to prevent illegal online transactions, the ambiguities around what constitutes "legal authority" or "illegal" could lead to arbitrary enforcement, which contravenes the legality and due process principles, both essential elements of the rule of law. From a cyber security perspective, the provision fails to address the underlying issues that may lead to unauthorized e-transactions, such as inadequate security measures.

RECOMMENDATIONS

Amend and restructure the cybercrime provisions to establish a more precise, detailed, and technologically contemporary cybercrime framework.

Modernize and differentiate cybercrime offenses based on harm, intent, and risk. The statute should clearly distinguish between different forms of cybercrimes — such as unauthorized access, unauthorized interference, data theft, malware deployment, phishing, ransomware, system disruption, and attacks against critical infrastructure — rather than aggregating diverse forms of conduct under broad offenses. Clear thresholds of harm, intent, authorization, and damage should be introduced, alongside graduated penalties reflecting the severity of the conduct and resulting impact. The framework should further provide explicit exemptions and safe-harbor protections for legitimate cybersecurity activities, including good-faith security research, vulnerability disclosure, penetration testing, and responsible security auditing conducted in accordance with recognized standards. Comparative frameworks such as the EU's *NIS2 Directive* and *Directive on Attacks Against Information Systems*, the United Kingdom's *Computer Misuse Act 1990*,

Singapore's *Computer Misuse Act 1993*, and Australia's *Cyber Security Act 2024* and *Security of Critical Infrastructure Act 2018* generally distinguish between different categories of cyber offenses and increasingly recognize the importance of protecting legitimate cybersecurity research, coordinated vulnerability disclosure, and defensive security activities.

Clarify the scope of gambling offenses and introduce differentiated liability. The statute should expressly define gambling and distinguish games of chance from games of skill, esports, fantasy sports, promotional competitions, and other legitimate digital activities. It should further differentiate between different actors, such as operators, organizers, facilitators, advertisers, intermediaries, and participants, with liability calibrated according to intent, knowledge, commercial benefit, and degree of involvement — penalties should be graduated based on scale, profit, repeat offending, and consumer harm, rather than applying a uniform framework across fundamentally different forms of conduct. Comparative frameworks such as the United Kingdom's *Gambling Act 2005*, Singapore's *Gambling Control Act 2022*, Australia's *Interactive Gambling Act 2001*, and other regimes adopted across the EU increasingly rely on licensing, consumer-protection, anti-money laundering, and risk-based regulatory models.

Clarify and narrowly define cyber forgery offenses. The statute should clearly distinguish cyber forgery from fraud, identity theft, unauthorized transactions, document manipulation, SIM-related offenses, and other forms of digital deception, while avoiding duplication across multiple provisions that criminalize substantially similar conduct. Comparative frameworks such as the EU *Directive on Combating Fraud and Counterfeiting of Non-Cash Means of Payment*, the United Kingdom's *Fraud Act 2006*, and Singapore's *Computer Misuse Act 1993* generally distinguish forgery-related conduct from broader cyber-enabled financial crimes and provide clearer doctrinal boundaries between forgery, fraud, and unauthorized access offenses.

Narrow and clarify the definition of cyber terrorism to align with internationally accepted thresholds. The statute should confine cyber terrorism offenses to conduct involving serious threats to national security, critical infrastructure, public safety, or human life, coupled with demonstrable terrorist intent. Vague concepts such as conduct that may affect friendly relations with foreign states or involve information that could potentially be used against state interests should be removed or substantially narrowed. The framework should clearly distinguish cyber terrorism from ordinary cybercrime, espionage, whistleblowing, journalism, academic research, public-interest disclosures, and lawful political expression, while introducing differentiated penalties based on intent, harm, and impact. Comparative frameworks, including the United Kingdom's *Terrorism Act 2000* and *Investigatory Powers Act 2016*, and Singapore's *Internal Security Act 1960 and Infrastructure Protection Act 2017* generally reserve terrorism offenses for conduct meeting high thresholds of intent, seriousness, and threat.

Reassess the utility, necessity, and scope of the unauthorized e-transaction offense to avoid duplication and regulatory overlap. Given the extensive body of directives, circulars, prudential standards, payment regulations, anti-money laundering requirements, and consumer protection measures issued by Bangladesh Bank governing both conventional and digital payment services and systems, the continued utility and necessity of a standalone criminal offense for unauthorized e-transactions should be reassessed. If retained, the provision should be narrowly tailored, clearly define concepts such as "legal authority," "authorization," and "unauthorized transaction," and expressly provide that it applies only where the conduct is not adequately addressed by existing banking, payment systems, fraud, anti-money laundering, cybercrime, or other sector-specific regulatory and criminal frameworks. This would reduce duplication, improve legal certainty, and minimize the risk of overlapping liability for substantially similar conduct.

PRIVACY

Sections 33, 34, 35 — Officers' investigative powers, and search, seizure, and arrest powers without warrant

ASSESSMENT

Broad investigative and enforcement powers conferred to investigating officers allow them to seize various forms of digital evidence and devices, as well as to arrest individuals, often without a warrant. Constitutional protections typically require that searches and seizures be conducted based on probable cause and aligned with well-defined protocols and oversight mechanisms but the provisions, as they stand, do not make these requirements a precondition, potentially infringing upon constitutional rights such as privacy, due process, and property protection. Absent clear guidelines on exercising these powers in a responsible, reasonable, proportionate, and transparent manner, and clear procedures for handling and securing seized data and devices, it may lead to overreach and abuse. Authority to seize digital devices and access stored data without robust and clearly defined safeguards can compromise sensitive information, including personal and business data unrelated to the offense under investigation.

RECOMMENDATIONS

Amend the privacy-infringing provisions to ensure alignment with procedural due process.

Strengthen safeguards governing investigative, search, seizure, and arrest powers. The statute should explicitly require that intrusive investigative measures — including searches, seizures of digital devices, access to stored data, and arrests — be subject to prior judicial authorization except in narrowly defined exigent circumstances, with any warrantless action requiring prompt judicial review. It should further establish clear thresholds of necessity, proportionality, reasonable suspicion, and relevance, alongside detailed procedures governing the collection, preservation, examination, retention, return, and destruction of seized devices and data. Additional safeguards should include minimization requirements for unrelated information, protection of privileged and confidential communications, chain-of-custody requirements, independent oversight, and effective remedies for unlawful searches, seizures, or arrests.

Sections 38, 39, 43 — Disclosure and secrecy obligations, and use of evidence in court

ASSESSMENT

Obligation on entities to mandatorily comply with request for information and assistance during an investigation without sufficient procedural safeguards and judicial review and oversight, while maintaining strict conditions of secrecy, under sections 38 and 39, potentially infringes on citizens' rights to privacy and due process, the constitutional protections against unreasonable searches and self-incrimination, as well as principles of transparency and accountability. Compounding these privacy concerns, section 43 allows

the admission of evidence obtained under the statute "notwithstanding anything contained to the contrary in the Evidence Act, 1872 (Act I of 1872) or any other law," eroding established evidentiary standards and due process guarantees embedded in traditional legal safeguards.

RECOMMENDATIONS

Amend the provisions to ensure disclosure and secrecy obligations are aligned with procedural due process.

Strengthen safeguards governing compelled disclosure, secrecy obligations, and admissibility of evidence. The statute should require that requests for information, assistance, disclosure of data, or other cooperation be subject to clearly defined legal thresholds, and, where appropriate, prior judicial authorization or independent oversight. Any secrecy obligations should be narrowly tailored and subject to challenge and review mechanisms, rather than operating as blanket restrictions. The law should further preserve core evidentiary and due process safeguards by clarifying that evidence obtained under the statute remains subject to principles of legality, reliability, authenticity, chain of custody, privilege, and procedural fairness, rather than broadly overriding the Evidence Act, 1872 and other applicable legal protections.

MISCELLANOUS

Section 29 — Personal liability for corporate non-compliances

ASSESSMENT

Contrary to the fundamental legal principle of the presumption of innocence enshrined in both constitutional and international human rights frameworks, section 29 reverses the burden of proof on company officials, requiring them to prove their innocence by demonstrating that the offense was committed without their knowledge or that they exercised due diligence to prevent it. It runs counters to the standard legal norms that the prosecution must prove the guilt of an accused person beyond a reasonable doubt. It disregards complexities of modern corporate operations, where decision-making and responsibility are often distributed across various levels of management and operational staffers. As a result, this could result in a chilling effect on corporate governance, discouraging skilled professionals from taking on leadership roles due to the heightened legal risks and officials becoming overly cautious, potentially stifling innovation and growth in sectors that rely on quick decision-making and risk-taking.

RECOMMENDATIONS

Amend the provision to align with established corporate and criminal law principles.

Align corporate liability provisions with principles of culpability, due process, and modern corporate governance. The statute should remove the reverse burden imposed on company officials and require the prosecution to establish the requisite elements of liability, including knowledge, intent, recklessness, negligence, or failure to comply with clearly defined statutory duties, in accordance with ordinary criminal law principles. Liability should be calibrated according to the individual's role, authority, degree of control, and involvement in the offending conduct, rather

than being presumed solely by virtue of holding a managerial or corporate position, while distinguishing between corporate liability and individual liability. The framework should further recognize and incentivize effective compliance programs, due diligence measures, internal controls, and risk-management systems. Comparative frameworks in jurisdictions such as the United Kingdom, Australia, Singapore, and the European Union increasingly favor fault-based and compliance-oriented approaches that preserve accountability without undermining the presumption of innocence, discouraging legitimate business activity, or imposing disproportionate liability on corporate officers.

Section 50 — Repealing Cyber Security Act, 2023, and quashing of cases under repealed cyber laws

ASSESSMENT

While expressly repealing the Cyber Security Act, 2023, the provision retains cases filed under non-speech-related provisions, while cases under speech-related provisions are deemed to be set aside under both the Cyber Security Act, 2023 and the Digital Security Act, 2018. However, the provision is notably silent on the status of the Information and Communication Technology Act, 2006, under which several speech-related cases have also been filed and may continue. Although cases under the repealed laws should stand set aside by operation of law without requiring further action, in practice many continue to proceed, with individuals remaining in pretrial detention until formal applications are filed by the accused for disposal of such cases.

RECOMMENDATIONS

Amend the case-disposal provision to ensure clarity around its operationalization.

Clarify the transitional framework and ensure effective implementation of case-disposal provisions. The statute should expressly address the status of proceedings initiated under all predecessor cyber laws, including the Information and Communication Technology Act, 2006, to eliminate uncertainty and ensure consistent treatment of similarly situated cases. Where the parliament intends for categories of cases to be discontinued, set aside, or otherwise benefit from transitional relief, such outcomes should occur automatically by operation of law without requiring affected individuals to initiate separate applications or proceedings. Where automatic effect is not intended, the framework should establish clear procedures, timelines, and institutional responsibilities for identifying, reviewing, dismissing, or otherwise disposing of affected cases, releasing individuals from pretrial detention where appropriate, updating criminal records, and notifying courts, prosecutors, prisons, and LEAs.

4. Bangladesh Telecommunication Act, 2001

After its amendment by the *Bangladesh Telecommunication Regulation (Amendment) Act, 2026*, the *Bangladesh Telecommunication Act, 2001* significantly expands its scope through broad definitions that extend beyond traditional infrastructure-based telecommunications providers that primarily offer transmission and connectivity services to include online intermediaries, over-the-top services, and internet-based platforms. This creates a regulatory conflation between infrastructure-based telecom operators and digital service providers. When read with mandatory licensing requirements, it introduces legal uncertainty as to whether such platforms must obtain telecommunications licenses — and if so, this would expose them to disproportionate compliance burdens, severe penalties, and enforcement risks.

The statute also introduces an expansive framework for surveillance, interception, and investigative powers. Centralized interception mechanisms allow broad state access to communications data, including content and metadata, while disclosure provisions enable compelled access to and public release of sensitive information. Despite formal safeguards, the breadth of powers, executive-dominated oversight, and broad exceptions both in this statute and others, such as the *Personal Data Protection Act, 2026*, raise concerns about normalization of surveillance and insufficient protection of fundamental rights, including privacy, freedom of expression, and association.

Finally, the institutional structure of the BTRC remains closely tied to the executive. Government control over appointments, removals, and sectoral policy, combined with the absence of an explicit guarantee of independence, limits its role as an autonomous regulator. This lack of institutional insulation, coupled with broad regulatory powers, raises concerns about accountability, transparency, and the risk of arbitrary or politicized enforcement.

We recommend retaining the *Bangladesh Telecommunication Act, 2001* in its pre-amendment form as the governance framework for traditional, infrastructure-based telecommunications services, while explicitly excluding online service providers, for which a separate online safety statute is proposed in Part B. We also recommend, in Part B, enacting a comprehensive statute on investigatory powers that more holistically addresses surveillance, interception, intelligence, and other law enforcement activities, anchored in clearly defined legal thresholds, prior judicial authorization, and robust procedural safeguards, thereby ensuring meaningful accountability of state authorities through independent oversight, transparency, and effective redress mechanisms.

SCOPE AND APPLICATION, POTENTIAL LICENSING REQUIREMENT

Sections 2, 3, 30 — Definition extending application to online service provider, with extraterritorial application and jurisdiction provisions

ASSESSMENT

Amended in 2026, the statute adopts expansive and imprecise definitions and confers authority on the BTRC that appears to extend its jurisdiction beyond traditional telecommunications operators to include online intermediaries and internet-based services within its regulatory purview. Specifically:

(i) Definition of "telecommunication" in section 2(11) broadly encompasses the transmission or reception of any form of speech, data, signals, information, or

expressions, while "telecommunication service" in section 2(15) extends beyond legacy carrier services to include internet-based services, AI, machine-to-machine and machine-to-human communications, and other emerging technologies. Although these definitions do not explicitly reference intermediaries, over-the-top services, or social media, such platforms are captured elsewhere in the statute (*see* below).

(ii) A newly introduced definition of "intermediary" in section 2(26a) broadly includes platforms that receive, transmit, store, process, or host electronic records, content, or communications on behalf of others via telecommunications networks or the internet, explicitly covering digital platforms such as video, streaming, broadcasting, payment, and content-based services.

(iii) A newly introduced definition of "over-the-top service" in section 2(2a) broadly includes applications or content delivered directly to end users over telecommunications networks or the internet without requiring dedicated infrastructure ownership.

(iv) Application of the statute is explicitly extended in section 3(1)(c) and (d) to any telecommunication services provided to and from Bangladesh, as well as to online social media, over-the-top services, and any "cell broadcasting-based" services.

Moreover, section 30(1)(j) empowers the BTRC to take necessary action in relation to intermediaries and social media intermediaries, including issuing directives, guidelines, and regulations.

When read together, particularly in light of the expanded definition of "telecommunication service" and the broad application and enabling provisions, these elements can be interpreted to bring online intermediaries, including social media platforms, streaming services, and AI-enabled services, within a regulatory framework traditionally designed for telecommunications carriers. This results in a regulatory conflation of functionally, operationally, and commercially distinct services, as platforms built on user-generated or curated content and data-driven models are treated equivalently to infrastructure-based telecommunications providers that primarily offer transmission and connectivity services. Such an approach fails to account for the layered architecture of the digital ecosystem and risks imposing disproportionate, ill-suited, and potentially duplicative regulatory obligations on online service providers.

In this context, provisions such as the mandatory licensing requirement under section 35(1) create significant legal uncertainty as to whether these platforms must obtain telecommunications licenses, potentially exposing them to inappropriate compliance burdens, enforcement risks, and penalties, despite their fundamentally different operational models.

RECOMMENDATIONS

Amend the provisions to distinguish between, and establish a differentiated framework for, telecommunication and internet-based services.

Clarify the scope of telecommunications regulation and maintain a clear separation between telecommunications services and internet-based services. The latest amendment to the statute should be revised so that it applies exclusively to traditional infrastructure-based telecommunications providers that primarily offer transmission and connectivity services. For the avoidance of doubt, the statute should specifically exclude online intermediaries, over-the-top services, social media platforms, search engines, and other internet-based platforms — and clarify that such excluded service providers are not subject to the telecommunication regime, and should not be treated as equivalent for licensing, compliance, enforcement, or regulatory purposes merely because they operate over telecommunications networks or because doing so may offer administrative or regulatory convenience. Their technical architecture, functions, risk profiles, and business models are fundamentally distinct from those of telecommunications carriers and therefore warrant separate and appropriately tailored regulatory frameworks.

Comparative practice adopts this differentiated regulatory model. For instance, in Australia, telecommunications infrastructure is regulated principally under the *Telecommunications Act 1997* and *Australian Communications and Media Authority Act 2005*, while online harms and platform-related obligations are governed separately under the *Online Safety Act 2021*. Similarly, in the United Kingdom, network and communications providers are regulated primarily under the *Communications Act 2003*, whereas user-generated content platforms and search services are regulated separately under the *Online Safety Act 2023*. Likewise, in India, telecommunications networks and spectrum are regulated under the *Telecommunications Act 2023*, while online intermediaries, social media platforms, and digital services are primarily governed through the *Information Technology Act 2000* and *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021* c. These frameworks recognize that digital platforms are not telecommunications carriers and should not automatically be subjected to telecommunications licensing and regulatory obligations solely because they use telecommunications infrastructure to deliver services. Bangladesh should adopt a similarly differentiated approach by confining telecommunications regulation to infrastructure and connectivity services, while regulating online intermediaries, over-the-top services, and other digital platforms through separate and appropriately tailored legal frameworks that reflect their distinct functions, risks, and societal impacts.

Sections 3, 35, 46, 61, 63, 76 — Licensing requirement and non-compliance risks, extraterritoriality, and enforcement authority

ASSESSMENT

Assuming that online service providers fall within the relevant definitions and statutory scope, the licensing and registration framework under the statute creates significant legal, operational, and compliance risks due to its breadth, severity, and lack of sector-specific differentiation. Specifically:

(i) A blanket prohibition exists in section 35(1) on providing telecommunication services without a license — and if this is extended to online service providers (such as social media platforms, streaming services, and AI-enabled services), it would expose them to a mandatory prior licensing regime designed for infrastructure-based telecom operators. This creates substantial entry barriers, particularly for global platforms and smaller digital service providers, and raises concerns about regulatory overreach and incompatibility with the open, cross-border nature of internet services.

(ii) A non-compliance with licensing requirements may attract, under section 35(2), up to ten years' imprisonment and penal fines reaching BDT 3,000,000,000. Additionally, section 63 provides for administrative fines reaching BDT 990,000,000, with an additional BDT 1,000,000 per day of continuing non-compliance. Particularly, section 3(1a) extends the application of the statute extraterritorially, providing that offences committed outside Bangladesh are punishable as if committed domestically, while section 76(1) imposes vicarious corporate liability by attributing offences to company officials (including directors, managers, employees, and representatives) unless they can demonstrate lack of knowledge or due diligence. When read together with section 76(2), it provides for expansive jurisdictional grounds for prosecution, allowing cases to be brought in multiple forums, including where the company operates, where the offence occurs, or where any company representative is located — thereby exposing online service providers and their officers, even in the absence of a physical presence in Bangladesh, to significant and potentially overlapping legal risks. Given the severity of penalties, this framework raises concerns regarding jurisdictional overreach, conflicts of law, and due process guarantees,

which, coupled with a reverse burden of proof, may have a chilling effect on business operations, investment, and the provision of cross-border digital services.

(iii) Overall, the severity of these penalties appears disproportionate, particularly when applied to platforms whose core functions do not involve spectrum use or network operation.

(iv) A non-compliance may also, under section 46, result in cancellation of license and appointment of administrators or receivers to take control of operations, which introduces significant regulatory uncertainty and risks of arbitrary or discretionary intervention, especially where licensing conditions are not clearly tailored to the operational realities of digital platforms.

(v) Enforcement powers under section 61 grant inspectors broad authority to inspect, access data, interrogate individuals, arrest without warrant, and seize equipment, creating heightened risks of coercive enforcement, business disruption, and intrusion into sensitive commercial and user data, particularly in the absence of clear procedural safeguards or judicial oversight.

Taken together, this framework creates a high-risk regulatory environment characterized by uncertainty, disproportionate liability, and expansive enforcement discretion, which may restrict market entry and undermine the growth of the digital ecosystem. It also raises concerns regarding due process, proportionality, and fundamental human rights, including privacy, freedom of expression, and protection against arbitrary state action, as well as alignment with international best practices.

SPEECH-RELATED OFFENSES

Sections 66, 66A — Content, signals, and calls that are false, or contrary to national unity and solidarity

ASSESSMENT

When applied to online service providers such as Facebook, WhatsApp, YouTube, or Netflix, these provisions extend the statute beyond its original remit, which was designed to regulate traditional telecommunications infrastructure and spectrum-based services, not content-driven, cross-border digital platforms. Specifically:

(i) It is an offence, under section 66, to intentionally send "false or fraudulent" messages, signals, or online content, as well as the possession or use of devices that may be used for such purposes, with penalties of up to five years' imprisonment and fines up to BDT 490,000,000. When applied to online platforms, this provision is ill-suited to the realities of user-generated content ecosystems, where platforms do not exercise prior control over communications, yet may face liability risks for content transmitted through their services.

(ii) A broad range of activities conducted through telecommunications or digital platforms — including acts affecting national security, public order, economic interests, hate speech, fraud, hacking, and disruption of communication systems — are criminalized under section 66A, with penalties of up to five years' imprisonment and fines up to BDT 990,000,000. The provision's expansive and vaguely defined scope risks capturing a wide spectrum of online conduct, including lawful expression, and does not reflect the distinct nature of platform-based harms, such as mis- and disinformation, cyberbullying, coordinated online abuse, or algorithmic amplification, which require more nuanced regulatory approaches.

While these provisions aim to address legitimate

harms such as fraud, incitement, and disruption of critical infrastructure and services, the application of telecommunications law to internet-based services is neither technically nor conceptually well-suited, nor proportionate to the nature and degree of involvement of such platforms compared to carrier service providers. It creates a structural mismatch: these platforms operate on user-generated or curated content models, often on a cross-border basis, without local infrastructure, and often without ex ante control over content, making compliance, attribution of liability, and enforcement inherently complex. In effect, these provisions reflect a category error in regulation, applying infrastructure-oriented telecommunications law to borderless, intermediary-based online services that operate on fundamentally different technical, operational, and commercial models.

Crucially, much of the conduct covered here is already addressed under the *Cyber Protection Act, 2026*, albeit under materially different definitions and penalty regimes, creating risks of duplication, parallel or overlapping proceedings across multiple forums (e.g., Cyber Tribunals under the *Cyber Protection Act, 2026*, and distinct regulatory and judicial processes under this statute), and potential misuse arising from overlapping jurisdiction and forum selection. Moreover, the use of vague and expansive terms across both provisions (e.g., "false or fraudulent" messages or "undermining economic interests") further increases the risk of subjective interpretation and selective enforcement, particularly in politically sensitive contexts, while raising concerns for freedom of expression. These provisions are not tailored to the specific dynamics of platform-based harms; instead, they rely on broad, punitive criminal sanctions that function as blunt instruments rather than targeted, proportionate regulatory tools.

RECOMMENDATIONS

Amend the provisions to distinguish between, and establish a differentiated framework for, telecommunication and internet-based services; and clarify that providers of internet-based services are not subject to telecommunications regulation and should not be treated as equivalent to telecommunications providers for licensing, compliance, enforcement, or other regulatory purposes. *See* our recommendation above.

SURVEILLANCE AND INTERCEPTION, INVESTIGATIVE POWERS

Sections 97A, 97B — Surveillance and interception

ASSESSMENT

While these provisions seek to establish a more detailed framework for surveillance and lawful interception, evidentiary use, and mandatory compliance obligations, however, taken together, they institutionalize a centralized surveillance architecture with broad scope, expansive state access, and limited independent oversight, raising concerns for fundamental rights.

(i) A centralized lawful interception regime, established under newly drafted section 97A, allows the monitoring, collection, storage, and analysis of a wide range of communications and data through a designated state-controlled platform under the Ministry of Home Affairs, accessible to multiple LEAs and Intelligence Agencies. Although subject to approval requirements and accompanied by a range of procedural safeguards intended to prevent misuse, the framework presents six key concerns

- *First,* given that the provision regulates surveillance activities (i.e., monitoring, collection, storage, and analysis) rather than the methods through which such activities may be conducted, it is sufficiently broad to encompass a wide range of interception and surveillance techniques, including audio and video recording, geolocation tracking, signal interception, facial recognition systems, laser microphones, metadata collection, browser tracking and cookies, spoofing, man-in-the-middle attacks, keylogging, deep packet inspection, cell-site simulators, phishing, scraping, browser fingerprinting, and platform monitoring. Such breadth, in the absence of clear statutory definitions, thresholds, safeguards, and limitations, risks enabling highly intrusive monitoring practices that may disproportionately interfere with fundamental rights, including privacy, freedom of expression, freedom of association, and confidentiality of communications, particularly where surveillance extends to lawful activities and communications unrelated to any genuine security threat or criminal conduct.

- *Second*, the framework must be read together with the *Personal Data Protection Act, 2026*, which affords sweeping exemptions to state agencies by waiving consent and other compliance obligations across broad and loosely defined categories such as public interest, national security, and crime prevention or law enforcement. Similarly, the newly introduced interception provision authorizes the government, or any agency designated by it, to undertake surveillance and interception activities on grounds of national security, public order, or serious crime notwithstanding anything to the contrary contained in any other law. When combined with longstanding concerns regarding institutional impunity, limited transparency, weak external oversight, and broad executive discretion, these exemptions and enabling provisions risk facilitating privacy-infringing conduct by state actors without meaningful accountability or effective remedies for affected individuals.

- *Third*, while the *Bangladesh Telecommunication Regulation (Amendment) Ordinance, 2026* originally included more robust safeguards, including prior authorization by an independent review council, the enacted framework substantially weakens this protection. The review council is no longer required to authorize surveillance or interception before it occurs, but instead performs only a post facto review function. Moreover, the law permits the government to designate a centralized interception authority while the NTMC continues to operate as the principal monitoring body, further consolidating surveillance capabilities within executive-controlled institutions.

- *Fourth*, the prior-authorization requirement is subject to a broad urgency exception, permitting interception and surveillance to be conducted without prior approval in cases of actual or perceived emergency. Notably, the enacted provision omits the requirement originally contained in the *Bangladesh Telecommunication Regulation (Amendment) Ordinance, 2026* to notify the relevant oversight authority within fourteen days following the exercise of emergency powers. In practice, if routinely invoked, this exception risks normalizing the bypassing of oversight mechanisms and substantially weakening an already constrained review process.

- *Fifth*, all service providers are required to provide technical assistance necessary to facilitate lawful interception. Although section 97A does not itself prescribe specific penalties for non-compliance, service providers remain subject to the broader enforcement framework of the statute, which includes significant administrative penalties, regulatory sanctions, potential suspension or revocation of licenses, and imprisonment. The absence of clear limits on the nature, scope, and proportionality of such assistance obligations may create operational, security, privacy, and compliance

challenges for service providers.

- Sixth, even assuming that courts, review bodies, and other procedural safeguards operate effectively and in good faith, the breadth of the permissible grounds for interception — including public order, national security, criminal investigation, prevention of serious crime, and protection of civilian lives — without clear statutory definitions, evidentiary thresholds, necessity requirements, or limiting criteria, significantly dilutes the effectiveness of those safeguards. The resulting discretion afforded to state authorities risks subjective interpretation and inconsistent application, undermining legal certainty, weakening oversight mechanisms, and ultimately compromising the integrity and legitimacy of the lawful interception framework.

(ii) Admissibility of intercepted information as evidence in court is provided in section 97B, while also allowing intelligence-derived information to remain outside formal evidentiary scrutiny. This creates a dual-use framework where certain surveillance outputs may influence investigations and proceedings while other information is carved out, creating risks of selective disclosure of inculpatory evidence while withholding exculpatory material, thereby raising concerns about fair trial rights and evidentiary integrity.

Collectively, these provisions entrench a formal, large-scale interception infrastructure, with implications for core fundamental rights, including privacy (through extensive surveillance, interception, data access, and retention practices), freedom of expression (through the chilling effects associated with actual or perceived monitoring), and freedom of assembly and association (through the capacity to monitor communications, networks, relationships, and collective activities). Over the past decade, Bangladesh has progressively expanded its surveillance capacity through a security-first regulatory approach. Available analyses, including a report by Tech Global Institute, estimate that Bangladesh spent nearly USD 190 million on surveillance technologies and spyware between 2015 and 2025; however, this likely represents only a portion of a broader and continuously evolving surveillance ecosystem, and the present framework risks further institutionalizing and expanding state surveillance capabilities without sufficiently robust, independent, and transparent oversight mechanisms. In May 2026, the cabinet reportedly approved USD 7.75 million for the procurement by NTMC of technologies to monitor, filter, and block online content, as well as manage large-scale network traffic across multiple data centres.

RECOMMENDATIONS

Repeal the surveillance and interception provisions, and enact a comprehensive Regulation of Investigatory Powers Act. *See* our recommendation in Part B.

Sections 84, 85 — Access to and disclosure of information by BTRC

ASSESSMENT

Ambiguous and overly broad provisions of section 84(2) enable BTRC to compel disclosure of any document and information, and "such other information as [BTRC] may consider necessary" from service providers and others, without clearly specifying the types of information that may be requested or the specific circumstances under which such information should be furnished, or any procedural guardrails or oversight mechanism — creating risks of arbitrary, disproportionate, and intrusive data demands that may infringe the right

to privacy and informational self-determination, and undermine principles of legality, necessity, and proportionality under constitutional and international human rights standards.

Specifically, sub-sections (1) and (3) of section 85 create heightened risks of privacy infringement and violations of data protection principles, as they enable BTRC to publicly disclose information obtained during investigations or proceedings — including sensitive personal data, communications data, trade secrets, proprietary technologies, intellectual property, and business information — without guaranteeing prior notice, meaningful opportunity to be heard, or effective remedies for affected parties. While a hearing is allowed before disclosure of confidential information, the broad and undefined discretion afforded to BTRC in determining "public interest" lowers the threshold for disclosure. Additionally, the absence of robust safeguards against unauthorized access, internal misuse, or third-party breaches heightens risks to the right to privacy, data security, and confidentiality of communications, with potential chilling effects on freedom of expression and association where individuals fear surveillance or exposure of their data.

For online service providers, these provisions create substantial legal and operational risks. Online platforms, particularly those handling large volumes of user-generated content and personal data across jurisdictions, may be compelled to disclose user information, communications metadata, or proprietary systems without clear limits or due process protections, potentially placing them in conflict with international data protection obligations, user privacy commitments, and encryption standards. The risk of compelled disclosure and public dissemination of sensitive data may also undermine user trust, deter platform usage, and expose providers to reputational, financial, and legal liabilities, while forcing them to navigate uncertain and potentially inconsistent compliance requirements in a highly discretionary regulatory environment.'

RECOMMENDATIONS

Amend the provisions to incorporate additional procedural safeguards governing BTRC's access to, use, retention, and disclosure of information.

Strengthen safeguards governing information requests, access, disclosure, and confidentiality. The statute should narrowly define the categories of information that may be requested, the purposes for which requests may be made, and the circumstances under which disclosure may be compelled, while requiring all requests to satisfy the principles of legality, necessity, proportionality, and data minimization. All requests for personal data, communications data, confidential business information, trade secrets, or other sensitive information should be subject to clear procedural safeguards, including written justification, independent authorization or oversight for intrusive requests, record-keeping requirements, and effective avenues for challenge and review. The statute should also substantially constrain the BTRC's authority to publicly disclose information by clearly defining "public interest," requiring prior notice and an opportunity to be heard, and limiting disclosure to what is strictly necessary.

Bangladesh Telecommunication Act, 2001

INSTITUTIONAL STRUCTURE

Sections 7, 9, 12, 32, 32A, 33, 34 — BTRC's institutional design and independence

ASSESSMENT

Over the past two decades, the institutional design of the BTRC has remained structurally and functionally subordinated to the executive branch, raising concerns regarding its independence. The government continues to retain decisive control over the composition of the BTRC, including the power to appoint and remove commissioners under sections 9 and 12, respectively, thereby undermining security of tenure and institutional autonomy. At the same time, the government, as well as the Ministry of Posts, Telecommunications and Information Technology, are vested with broad authority over policy formulation, rule-making, coordination, supervision, and implementation in the telecommunications sector, which significantly constrains the BTRC's role as an independent regulator. Even internal accountability mechanisms, such as the proposed transparency and accountability committee constituted under newly introduced section 32A(7), despite including a mix of state and non-state representatives, are constituted by and remain subject to government control. Notably, unlike other provisions in this statute — such as the constitution of the proposed review council — there is no explicit requirement that the BTRC function independently from administrative, political, or institutional influence, reinforcing concerns that it operates without meaningful insulation from executive control.

RECOMMENDATIONS

Amend the provisions to ensure regulatory independence, accountability, and transparency for BTRC.

Establish a more independent, accountable, and transparent governance framework for the BTRC. The statute should expressly guarantee the institutional, operational, financial, and decision-making independence of the BTRC, while clearly distinguishing the government's role in setting high-level telecommunications policy from the regulator's role in licensing, supervision, enforcement, and dispute resolution. Appointment and removal processes for commissioners should be transparent, merit-based, and subject to objective statutory criteria, fixed terms, security of tenure, and safeguards against arbitrary removal. Additionally, internal oversight bodies, including any transparency and accountability committees, should operate independently and not be subject to executive control in their composition or functioning. The statute should further require public consultation, reasoned decision-making, periodic reporting, parliamentary scrutiny, conflict-of-interest safeguards, and independent review mechanisms to enhance accountability and public trust. Comparative practice increasingly favors independent communications regulators insulated from routine political influence, including the United Kingdom's Ofcom, Australia's Australian Communications and Media Authority, and telecommunications and electronic communications regulators across the EU. Bangladesh should adopt a similar model to ensure that telecommunications regulation remains transparent, predictable, technically informed, and free from undue political or administrative interference.

5. Penal Code, 1860

Certain provisions of the *Penal Code, 1860* retain colonial-era features that are increasingly misaligned with constitutional guarantees, international human rights standards, and contemporary digital realities. These provisions — particularly those criminalizing speech (e.g., sedition, public order, religious offenses, defamation, and student political participation) — are characterized by overbreadth, vague drafting, low thresholds of liability, and disproportionate penalties, creating risks of arbitrary enforcement and chilling effects on free expression, political participation, and engagement online. Additionally, certain non-speech elements, such as those criminalizing common and legitimate commercial practices within the digital economy, reflect outdated regulatory approaches that undermine innovation and economic development. Overall, the provisions identified suffer from conceptual incoherence, duplication with newer laws, and failure to address modern harms effectively. Accordingly, we recommend repealing such provisions, specifically decriminalizing speech-related offenses, enacting targeted, standalone legislation addressing specific harms, and strengthening sector-specific regulatory frameworks to address contemporary challenges in a rights-respecting and proportionate manner.

SPEECH-RELATED OFFENSES

Expressions, including words, signs, and representation, criminalized under the statute includes:

- ***(A) sections 123A, 124A — sedition, and condemning creation of Bangladesh and expressions against its sovereignty***
- ***(B) sections 153A, 505(c), 505(d) — inciting or promoting enmity between classes of citizens***
- ***(C) sections 295A, 298 — outraging or wounding religious feelings of any class***
- ***(D) sections 505(b), 505A — offense against the state, national security, public order, or foreign relations***
- ***(E) section 153B — induction or attempted induction of students and educational institutions into political activities***

ASSESSMENT

As remnants of a colonial past, most of these provisions were originally introduced during the nineteenth century or incorporated through subsequent amendments such as the *Indian Penal Code Amendment Act, 1898* (Act No. IV of 1898) and the *Pakistan Penal Code (Amendment) Act, 1950* (Act No. LXXI of 1950). One exception is section 505A, which was introduced through the *Penal Code (Amendment) Act, 1991* (Act No. XV of 1991) after the post-military transition and reestablishment of parliamentary democracy in the 1990s.

Despite their historical origins, these provisions are now outdated and counterproductive, suffering from severe overbreadth and vagueness while carrying significant penalties. Specifically, the expansive language of the provisions extends their applicability to online expressions, including social media content, blogs posts, and other digital communications, raising concerns about free speech and privacy. Such overbroad criminalization also violates the principle of legal certainty and undermines the rule of law. Moreover, the heavy-handed penalties, including life imprisonment, fail to meet the constitutional requirement that restrictions on fundamental rights be both reasonable and

necessary in a democratic society. Chilling free speech and public discourse runs counter to the high ideals for a vibrant democracy enshrined in the Constitution.

(A) From a legal standpoint, these provisions use undefined and ambiguous terms — such as "prejudicial to the safety" and "endanger the sovereignty" of Bangladesh in section 123A, exciting "disaffection" against the government in section 124A, causing "enmity," "hatred" and "ill-will" between different classes of the citizens in sections 153A and 505(d), and "outraging" and "wounding" religious feelings in sections 295A and 298. Similarly, the terms "prejudicial to the interests of the security of Bangladesh," "maintenance of friendly relations with foreign states," and "maintenance of supplies and services essential to the community" in sections 505(b) and 505A are not clearly defined, leaving room for wide-ranging interpretation.

Given the dangerously low threshold — with mere attempts or likelihood itself constituting an offense with severe penalties, including life imprisonment — the provision not only makes it difficult for individuals to distinguish between lawful expression and criminal conduct but also creates avenues for arbitrary, subjective, and inconsistent interpretations and enforcement by law enforcement and judicial authorities, often resulting in the prosecution of individuals for simply expressing dissent or criticism online.

Over-criminalization of speech under these provisions, especially related to sensitive issues related to government policy, international relations, public services, or national history, fails to address the root causes and hinder efforts to promote genuine dialogue and understanding between different stakeholders. Globally, many countries have either repealed or significantly narrowed the scope of discretionary legal provisions, making the retention of such draconian measures in Bangladesh a poor reflection of the country's commitment to democratic principles and human rights, both online and offline.

(B) See the comments in (A) above.

(C) See the comments in (A) above.

(D) See the comments in (A) above.

(E) Criminalization of inducing or attempting to induce students into engaging in political activities that may disturb or undermine public order is overbroad and vague, lacking clear definitions for key terms such as "disturb" or "undermine" public order, or "take part in any political activity," thereby creating ambiguity about what constitutes unlawful political activity for students.
A low threshold for criminal liability — where even an attempt to induce political activity can lead to imprisonment — exacerbates these concerns, as it allows for pre-emptive and punitive actions against individuals or groups based on subjective interpretations of their intentions or actions. Where such political activity is primarily speech-based, the provision directly engages core constitutional protections. Constitutionally, the provision infringes on the rights to freedom of speech, assembly, association, and equality and non-discrimination, as well as safeguards against arbitrary arrest and detention.

Criminalization of political expression and participation among students, a demographic historically at the forefront of positively shaping democratic governance in Bangladesh through political engagement and activism, is in direct conflict with the constitutional pledges of a democratic society where political, economic, and social equality and justice are secured for all citizens. However, more problematically, the policy rationale behind criminalizing the inducement of students to engage in politics, while not prohibiting students themselves from participating in political activity and discourse, is internally inconsistent, since, if students are permitted to participate in political activities and discourses, banning their recruitment or encouragement to participate serves no logical objective and undermines democratic participation.

As much of the political discourse and mobilization among students occurs online, the provision

poses a threat to freedom of expression in digital spaces. Furthermore, the provision could be used to rationalize state-sanctioned monitoring and censorship in situations considered politically sensitive or potentially disruptive to public order. Overall, this restriction is unreasonable and counterproductive, as, instead of nurturing an informed and active citizenry, it undermines the development of political awareness and promotes political apathy, which is detrimental to democracy itself.

RECOMMENDATIONS

Delete the provisions.

Repeal archaic provisions restricting fundamental right to freedom of expression. Outdated provisions criminalizing various forms of expression under these provisions, which may have once been reasonable to maintain control over a subjugated population, now stand in direct tension with the constitutional commitment to "*realise through the democratic process a socialist society, free from exploitation a society in which the rule of law, fundamental human rights and freedom, equality and justice, political, economic and social, will be secured for all citizens.*" The continued retention of overbroad, undefined, and vague offenses, coupled with disproportionate penalties, undermines legal certainty and fails to meet the constitutional and international human rights standards of legality, necessity, and proportionality, while also creating conditions for arbitrary enforcement and chilling lawful expression.

Globally, many countries have moved to repeal or significantly narrow such provisions. For instance, the United Kingdom abolished the offenses of sedition and seditious libel in England and Wales and in Northern Ireland (*see* section 73 of the *Coroners and Justice Act 2009*), as the common law offense, initially introduced to suppress dissent against the monarchy, was considered outdated and inconsistent with the values of free speech in a modern democracy. Similarly, New Zealand and Singapore repealed sedition (*see* the *Crimes (Repeal of Seditious Offences) Amendment Act 2007* and the *Sedition (Repeal) Act 2021*). Instead, the legal frameworks of these countries shifted toward more targeted frameworks addressing specific harms such as terrorism or hate speech rather than broad restrictions on dissent. In contrast, countries such as India and Australia have largely retained the substance of sedition-type offenses under revised nomenclature, offering limited reform value and highlighting the risks of cosmetic legislative change without substantive rights protections (*see* the *Bharatiya Nyaya Sanhita, 2023* and the *National Security Legislation Amendment Act 2010*), and are poor examples to follow.

A similar global trend is evident in the decriminalization of blasphemy, with countries such as Ireland, Denmark, Iceland, and Canada repealing such offenses in recognition of their incompatibility with freedom of expression in pluralistic societies (*see* the *Thirty-Seventh Amendment of the Constitution (Repeal of Offense of Publication or Utterance of Blasphemous Matter) Act 2018*, the *Law on Amending the Penal Code, Law No. 675*, the *Act Amending the General Penal Code, no. 19/1940*, and the *Act to Amend the Criminal Code and the Department of Justice Act and to Make Consequential Amendments to another Act*).

While many jurisdictions retain provisions related to incitement to offense, the scope is typically narrowly defined and accompanied by procedural safeguards. For example, in the United Kingdom, incitement to certain offenses, such as hatred based on race, religion, and sexual orientation, is an offense, but both the provisions and the sanctions are narrowly tailored, and sufficient procedural guardrails exists to prevent abuse (*see* the *Public Order Act 1986*, the Code for Crown Prosecutors on Public Order Offences and Racist and Religious Hate Crime, and the Sentencing Guidelines on Public Order Offences). A higher threshold is required for prosecution — conduct must be threatening, abusive, or insulting, and it has to be intended or likely to stir up racial hatred. However, prosecutions are subject to layered oversight and institutional checks: the prosecutor must first assess the rights of the individual to freedom of expression against the duty of the state

to act proportionately in the interests of public safety, to prevent disorder and crime, and to protect the rights of others; thereafter, the allegation must be referred to the Special Crime & Counter Terrorism Division, who will only proceed with prosecution on receipt of consent of the Attorney General. Adoption of such a standardized and systemic approach ensures fair trial for the accused.

Repeal archaic provisions restricting fundamental right to political participation. While a few countries, such as South Korea, maintain laws that limit certain political activities (particularly those linked to national security or pro-North Korea ideologies), these restrictions are narrowly tailored and do not impose a broad prohibition on student political engagement itself (*see* the *National Security Act*). In contrast, section 153B — introduced during the active political engagement of students in the erstwhile East Pakistan, especially during the 1962 East Pakistan Education Movement — imposes a prohibition on the inducement of students into politics, creates a constitutional conundrum: it does not disallow students to engage in political activity and discourse, but targets the process of encouraging or facilitating such participation.This distinction is not only an unreasonable restriction on freedoms of expression, assembly, and association, but also functionally incoherent and difficult to enforce in practice, thereby undermining both legal clarity and democratic participation.

Sections 499, 500 — Criminal defamation

ASSESSMENT

While section 499 outlines ten exceptions that ostensibly protect the constitutional right to free speech, these are insufficient to counterbalance the broad and punitive scope of criminal defamation. Exceptions such as imputations of truth for the public good or commentary on the conduct of public servants are narrowly construed and subject to variable judicial interpretation, and, therefore, do little to mitigate the overarching threat to freedom of expression.

Even the penalty regime, which entails imprisonment for up to two years and/or fines without clear statutory limits or guidance, is disproportionately harsh; this has a chilling effect on free speech and the free flow of information, deterring individuals — from ordinary citizens, journalists, and intellectuals to political opponents and activists — from speaking out on matters of public interest for fear of legal retribution, thereby undermining an informed and engaged citizenry essential to democratic governance.

Criminal defamation regimes are increasingly out of step with the realities of the digital communication ecosystem: while the rapid dissemination of information is crucial for democratic participation and accountability, the speed and reach of digital platforms also increase the potential for defamation claims. This risks undermining the role of the internet as a platform for open and democratic discourse by expanding liability for lawful expression across a wide range of actors. Further compounding the risk of abuse is the absence of robust safeguards against wrongful prosecution and the lack of clear guidelines for law enforcement. As a result, criminal defamation is widely regarded as inconsistent with international human rights standards, with many countries increasingly favoring civil remedies over criminal sanctions.

RECOMMENDATIONS

Delete the provisions.

Decriminalize defamation, and replace it with civil remedies. The global trend among democratic countries, and international human rights standards endorsed by the United Nations Human Rights Committee and the European Union Parliamentary Assembly of the Council of Europe, has been to shift away from criminal defamation toward administrative or civil remedies as a more appropriate and balanced response to defamation claims, provided that such remedies have a less punitive effect than those of criminal law (see General Comment No. 34, PACE Resolution 1577, and Commission Recommendation (EU) 2022/758; see also the Council of Europe's study on the alignment of laws and practices concerning defamation with the relevant case-law of the European Court of Human Rights on freedom of expression, particularly with regard to the principle of proportionality in 2012 and Freedom of Expression and Defamation: A Study of the Case Law of the European Court of Human Rights in 2016, and the Organization for Security and Cooperation's special report on legal harassment and abuse of the judicial system against the media in 2021). Such an approach reflects a shift toward proportionate, rights-respecting regulation of speech-related harms. Civil remedies, such as compensation for damages, allow for more proportionate and context-sensitive responses, enabling balanced adjudication through compensation and rectification of reputational harm, without unduly restricting the fundamental right to free expression.

Section 509 — Insulting women's modesty

ASSESSMENT

While the intent underscoring this provision — to protect women from harassment and safeguarding their dignity — is legitimate, its reliance on undefined and vague terms such as "modesty" and "insult," coupled with its origins in nineteenth-century colonial legal frameworks, renders it outdated and ill-suited to contemporary constitutional and social contexts. At the time of its enactment, prevailing patriarchal norms perceived women as the primary, and often only, group vulnerable to harassment, reinforcing a paternalistic framework of protection and reflecting a limited understanding of vulnerability and gender roles. Similarly, the concept of "modesty" is rooted in colonial-era understanding of morality, reflecting rigid and gendered expectations of behavior based on the belief that women's virtue and dignity must be policed and protected.

Furthermore, such vague terminology invites subjective interpretation by law enforcement and the judiciary, which undermines the principle of legal certainty. In the context of contemporary digital environments, where interactions are diverse, informal, and rapidly evolving, this ambiguity risks enabling selective enforcement and suppression of lawful expression online. Moreover, its broad scope may inadvertently legitimize intrusive regulation of personal behavior, reinforce gender stereotypes, and constrain individual autonomy, which is inconsistent with modern constitutional values. This may also discourage women from participating in public and digital discourse due to fear of legal consequences.

A provision anchored in "modesty" is inadequate to address the evolving and multifaceted nature of harassment, which increasingly occurs across both offline and online spaces and affects a broader range of individuals. A more effective approach would involve enacting clear, narrowly defined, and context-sensitive legal provisions that specifically address harassment, stalking, and violence against women and other vulnerable groups, including transgender and intersex individuals and minorities, in a manner that is consistent with principles of legality, proportionality, and equality.

Penal Code, 1860

RECOMMENDATIONS

Delete the provision, and introduce a standalone law on harassment and abusive behaviors.

Enact standalone, gender-neutral, inclusive legislation against online and offline abuses. Reform of isolated, colonial-era provisions is insufficient to meet contemporary policy objectives; instead, there is a need for a standalone, comprehensive statute that addresses harassment in all its forms, aligned with the principles of human dignity, gender equality, and human rights.

The existing legal framework in Bangladesh, including sector-specific provisions and judicial guidelines (such as the *Prevention of Women and Children Repression Act, 2000*, and the decision of the High Court Division in *Bangladesh National Women Lawyers Association v. Bangladesh*), remains fragmented and insufficient to address the full spectrum of harassment across contexts and mediums. The proposed statutory framework should therefore provide comprehensive and universal protection against abuse, both online and offline, particularly for women, transgender individuals, LGBTQ communities, minorities, and other vulnerable groups, while ensuring that protections are extended equally to all citizens, regardless of sex or gender identity.

Such legislation should avoid vague, subjective terms that can lead to arbitrary enforcement, and instead clearly define distinct categories of abusive conduct, particularly in digital environments, including cyberstalking, cyberbullying, doxxing, trolling, catfishing, sextortion, flaming, cyber grooming, identity theft, hacking, revenge porn, non-consensual intimate image sharing, online hate speech, media manipulation, and other forms of technology-facilitated abuse. This approach would enhance legal certainty, enable proportionate enforcement, and better reflect the evolving nature of harm in digital ecosystems. While the *Cyber Protection Act, 2026* criminalized many of these conducts, it remains inadequate (see Part B).

As affirmed by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, and echoed by the Human Rights Council, individuals' rights must be afforded equal protection online and offline, and states have a duty to enact legislation to protect individuals from abuse in the digital sphere (see A/HRC/38/35 and Resolution 38/7).

NON-SPEECH OFFENSES

Section 294B — Offering prizes or rewards

ASSESSMENT

Criminalization of incentives, such as rewards, discounts, and promotional offers, was introduced by the Pakistan Penal Code (Amendment) Act, 1965 (Act No. XX of 1965). While this approach may have reflected legitimate regulatory concerns in a predominantly physical and localized economy with limited consumer protection frameworks in the twentieth century, it is no longer aligned with contemporary market realities. In contrast, incentive-based models are now standard, legitimate, and often essential components of digital business strategies used to drive user engagement, competition, and innovation. In practice, this could extend to a wide range of commonplace commercial activities, including discount codes, cashback offers, loyalty programs, in-game rewards and virtual currencies, and promotional campaigns on digital platforms — all of which are integral to user acquisition, engagement, and retention in the digital economy. This disconnect between outdated legal norms and current market practices increases the likelihood of widespread non-compliance

and regulatory inefficiency. Accordingly, the provision risks creating a restrictive regulatory environment that may deter innovation, constrain market participation, and undermine broader policy objectives relating to digital transformation and economic growth. Constitutionally, the provision's vague drafting and expansive scope create significant risks of arbitrary interpretation and selective enforcement, infringing core principles of legal certainty and due process, as businesses cannot reasonably be expected to comply with laws that are misaligned with contemporary commercial practices, as well as constitutional guarantees of equality before the law and the freedom to engage in trade, business, and profession.

RECOMMENDATIONS

Delete the provision.

Decriminalize legitimate commercial practices, and strengthen existing consumer and financial crimes laws. This provision, being archaic and misaligned with contemporary economic and legal frameworks, should be repealed insofar as it criminalizes legitimate commercial practices. At the time of its introduction, consumer protection laws were underdeveloped, and there was a strong need for regulation to curb misleading promotions and ensure fairness in commerce. However, the economic and legal landscape has dramatically evolved since then. Accordingly, regulatory focus should shift toward strengthening regulations on deceptive or illegal practices, such as misrepresentation, false inducement, and fraudulent financial schemes, as well as modern financial issues like cryptocurrency regulation and the prevention of financial crimes. Sector-specific and financial regulatory frameworks, although currently underdeveloped and requiring substantive strengthening to effectively respond to evolving market practices and financial risks, are more appropriate vehicles to address these concerns in a targeted and proportionate manner.

6. Pornography Control Act, 2012

The *Pornography Control Act, 2012* adopts an outdated and expansive regulatory approach that criminalizes broadly and vaguely defined categories of pornographic materials, without sufficiently distinguishing between consensual adult content and exploitative or abusive sexual harms such as CSAM, TFSV, and non-consensual pornography. The framework combines vague definitions, disproportionate penalties, broad search and seizure powers, and inadequate differentiation between varying degrees of harm and culpability, creating risks of arbitrary enforcement, legal uncertainty, and over-criminalization. At the same time, the statute reflects an outdated understanding of contemporary pornography ecosystems, which are now predominantly platform-mediated, transnational, encrypted, algorithmically distributed, and increasingly user-generated, including through live-streaming and subscription-based adult content services. Significant overlap with section 25 of the *Cyber Protection Act, 2026* further creates doctrinal inconsistency, conflicting penalty structures, and risks of arbitrary prosecutorial discretion.

From a constitutional, human rights, and policy perspective, several provisions risk disproportionately interfering with rights relating to privacy, freedom of expression, due process, and fair trial guarantees. Criminalization of possession and storage of consensual adult content for private, non-commercial purposes — combined with cognizable and non-bailable offenses and extensive law enforcement powers — creates risks of invasive surveillance, selective enforcement, and abuse. More broadly, the current framework risks diverting regulatory and enforcement resources away from genuinely harmful conduct, such as CSAM, TFSV, non-consensual intimate imagery, and trafficking-related exploitation, which increasingly constitute the primary online sexual harms requiring urgent intervention.

Accordingly, to avoid overlapping criminalization and duplicative offenses across multiple statutes, either the statute should be repealed and replaced with a comprehensive and technologically contemporary online safety statute, as proposed in Part B, capable of coherently regulating the broader ecosystem of pornography, online sexual exploitation, and technology-facilitated sexual harms, or it should be substantially amended by introducing a narrower, harm-based, and rights-respecting regulatory approach as recommended here. Such reforms should introduce clearer and more objective definitions, differentiate between consensual adult content and exploitative sexual abuse material, modernize the framework to reflect contemporary digital distribution ecosystems, establish proportionate enforcement and sentencing mechanisms, and strengthen procedural safeguards, intermediary liability protections, and cross-border enforcement cooperation.

DEFINITIONS

Section 2(c) — Definition of "pornography"

ASSESSMENT

The current definition of "pornography" is vague and overly broad, criminalizing a wide range of materials that may not be intended to be pornographic. Without clear definitions or explanations, subjective and ambiguous terms like "sexually suggestive," "obscene," "semi-nude" and "sexually arousing" materials risk arbitrary enforcement and overreach. Additionally, the definition reflects and reinforces cultural and moral biases that may not be universally shared or accepted, especially with the rapidly evolving nature of digital media, where the distinction between pornographic and non-pornographic material is not binary. The definition

not only infringes freedom of expression but also violates the constitutional principle that restrictions on fundamental rights must be clearly defined, narrowly tailored, necessary, and reasonable. As currently framed, the provision fails to provide a clear and objective standard for what constitutes pornography, making it difficult to distinguish between protected and unprotected content.

By casting such a wide net, the law may suppress legitimate online expression, including discussions about sexual health, education, and rights, or satirical content. Exemptions for artistic and educational works (and religious materials under section 9) are narrowly framed and do not reflect the diverse purposes for which sexually explicit material may be created or consumed, including, for instance, literary, research, artistic, political, cultural, historical, religious, educational, media reporting, criminal investigation, medical, or scientific value or purpose. A limited set of exemptions, and their subjective interpretation, makes the statute susceptible to abuse and inconsistent application. It creates legal uncertainty for content creators, publishers, and distributors, who may be unsure whether their work falls within the prohibited categories, as well as for individuals challenging conventional social norms or exploring themes related to sexuality, gender, or identity, thereby creating leeway for targeted enforcement against individuals for personal or political reasons.

Furthermore, the definition reflects an outdated understanding of pornography consumption; today, pornography is predominantly consumed through web-based services, social media platforms, live-streaming, user-generated adult content platforms, interactive platforms, and other emerging digitally mediated forms of sexual content production and distribution, all of which are conspicuously absent from this definition. As a result, the provision is both overbroad in some areas and underinclusive in others, making it ill-suited to regulate contemporary forms of online pornography. This creates legal and logistical implementation challenges, as LEAs will struggle to effectively monitor and regulate the vast amount of content that could potentially fall under this broad definition. This could divert resources away from more serious crimes or lead to selective enforcement that targets specific groups or individuals.

Additionally, the inclusion of “soft versions” of pornographic materials in the definition creates ambiguities around whether it refers to less explicit soft-core pornography or to digital formats of pornographic material. This lack of clarity could lead to confusion in both legal interpretation and enforcement.

Given that the *Pornography Control Act, 2012* is intended to operate as the special law governing pornography-related offenses, core definitions, including those relating to non-consensual pornography and child sexual abuse material, should ideally be comprehensively and coherently defined within this framework itself, with other statutes cross-referencing or harmonizing with those definitions where necessary. However, the current framework suffers from substantial overlap and doctrinal duplication with section 25 of the *Cyber Protection Act, 2026*, which separately criminalizes conduct relating to revenge porn and child sexual abuse material, both of which not only fall within the broad definition of “pornography” under this statute but are themselves either underinclusive, conceptually outdated, or excessively broad and structurally incoherent. As a result, the same underlying conduct may potentially be prosecuted under two separate statutory frameworks carrying materially different penalty regimes, raising concerns regarding legal certainty, coherent legislative design, proportionality, and protection against arbitrary or selective prosecutorial discretion.

RECOMMENDATIONS

Amend the definition, and introduce definitions for specific types of harmful pornographic content.

Clarify and narrowly tailor the definition, providing clear and objective standards. Definition should exclude vague terms — like "sexually suggestive," "obscene," "semi-nude," and "sexually arousing" — to eliminate ambiguity and subjectivity in interpretation and enforcement. For instance, the term can be defined as:

> *""pornography" means any material or content, in any medium, that expressly and predominantly depicts or describes, of or related to a person, any real or simulated sexually explicit acts, or any sexually explicit communication, or any sexual organs, or any sexual exploitation or abuse, or any sexual services, which lacks significant literary, research, artistic, political, cultural, historical, religious, educational, media reporting, law enforcement or criminal investigation, medical, or scientific value or purpose; and it is immaterial for these purposes whether such material is intended to cause or provoke sexual arousal or gratification, but excludes child sexual abuse material, non-consensual pornography, or digitally created pornography"*

Abovementioned proposed definition provides a clear and enforceable framework by specifying objective components that enable the unambiguous identification of harmful content.

Firstly, the phrase "any material, in any medium" ensures comprehensive coverage across all platforms and forms of expression, including digital, print, audio, or visual formats.

Secondly, the term "expressly and predominantly" enables targeting of content where the sexual acts or organs are the primary focus, preventing misclassification of incidental, contextual, or peripheral depictions of sexual or sexualised content.

Thirdly, the exclusion of intention in the definition — that is, a content is pornographic irrespective of whether it is intended to cause sexual arousal or gratification, thereby offering objective assessment criteria to classify pornography and avoiding the subjective challenge of determining intent — ensures that content is regulated based on its nature rather than the intentions of the creators, publishers, and distributors.

Fourthly, the exclusions in respect of certain content (such as literary, artistic, cultural, religious, and scientific) enables protection for content that serves a legitimate purpose, safeguarding freedom of expression in cases where sexual content contributes meaningfully to public discourse, education, or creative work.

Finally, certain categories of explicit materials, including CSAM and TFSV, should be expressly excluded from the general definition, and separately defined, to avoid uniform treatment of different types of pornographic materials, and enable differentiated and contextual enforcement against these more harmful content.

This combination of elements creates a precise, objective, and enforceable definition that helps identify harmful pornography without overreaching into protected speech.

Distinguish between harmful and non-harmful content. While moral reservations based on subjective assessment about pornography in Bangladesh is not uncommon, distinction must be drawn between harmful pornography (e.g., CSAM and TFSV) and non-harmful, consensual adult content, in order to focus enforcement on content that poses genuine or greater harm to individuals and society.

Specifically, these harmful categories of pornography should be explicitly defined, for instance, as:

> *(1) ""child sexual abuse material" means any material, content, or representation, in any medium, that:*
>
> *(a) visually, audibly, or textually, or otherwise, depicts or describes:*
>
> *(i) any real or simulated sexually explicit acts, or*

(ii) any sexual organs in a sexually explicit context, or
(iii) sexual exploitation or abuse, or sexual services,
(iv) sexually explicit communication with another person, including a child, or
(v) sex offenses as defined under the applicable laws,

of, or related to, or in the presence of, any child (as defined in sections 2(17) and 4 of the Children Act, 2013 (Act No. XXIV of 2013), or

(b) visually, audibly, or textually, or otherwise, causes, incites, encourages, or instructs any child to:

(i) engage in, or observe, any real or simulated sexually explicit acts, or
(ii) expose any sexual organs in a sexually explicit context, or
(iii) engage or assist in sexual exploitation or abuse, or sexual services, or
(iv) engage in, or observe, sexually explicit communication with another person, including a child, or
(v) engage or assist in other sex offenses as defined under the applicable laws, including paying or getting paid for sexual services, controlling a child for sexual exploitation, or grooming a child for sexual purposes, or

(c) visually, audibly, or textually, or otherwise, causes, incites, encourages, or instructs any person to facilitate or arrange for, or cause, any child to:

(i) engage in, or observe, any real or simulated sexually explicit acts, or
(ii) expose any sexual organs in a sexually explicit context, or
(iii) engage, or assist, in sexual exploitation or abuse, or sexual services, or
(iv) engage in, or observe, sexually explicit communication with another person, including a child, or
(v) engage or assist in other sex offenses as defined under the applicable laws, including paying or getting paid for sexual services, controlling a child for sexual exploitation, or grooming a child for sexual purposes;

provided that it is immaterial for these purposes whether such material is intended to cause or provoke sexual arousal or gratification;

and further provided that any material demonstrably created and/or used strictly for, and only for, legitimate purposes in the relation law enforcement or criminal investigation, medical treatment, or authorized research, education, or media reporting purposes shall not fall within this definition"

(2) ""non-consensual pornography" means any material or content, in any medium, that depicts or describes, of or related to a person, any real or simulated sexually explicit acts, or any sexual organs in a sexually explicit context, or any sexual exploitation or abuse, or any sexual services, where one or more depicted persons has not given clear, informed, and voluntary consent for recording, production, marketing, dissemination, purchase, sale, or display of such material, as applicable; and it is immaterial for these purposes whether such material is intended to cause or provoke sexual arousal or gratification;

provided that any material demonstrably created and/or used strictly for, and only for, legitimate purposes in the relation law enforcement or criminal investigation, medical treatment, or authorized research and education purposes shall not fall within this definition"

(3) ""digitally created pornography" means any pornography, child sexual abuse material, or non-consensual pornography that has been created using, or with the assistance of, any artificial intelligence or other digital tools and technologies, expressly and predominantly depicting or describing, of or related to a real person, the likeness of such person, in any sexually explicit acts, or any sexually explicit communication, or sexual organs in a sexually explicit, or any sexual exploitation or abuse against or involving them, where one or more depicted persons has not given clear, informed, and voluntary consent for the creation of such material; and it is immaterial for these purposes whether such material is intended to cause or provoke sexual arousal or gratification;

> *provided that the term "create" and its variants shall include, without limitation, the act of generating, modifying, manipulating, synthesizing, superimposing, or otherwise altering any digital or visual material or representation to resemble or depict a real person, including deepfakes and cheapfakes, regardless of whether such likeness was originally derived from a real image or generated entirely through digital means;*
>
> *provided further that any material demonstrably created and/or used strictly for, and only for, legitimate purposes in the relation law enforcement or criminal investigation, or authorized research, education, or media reporting purposes shall not fall within this definition"*

Each of these definitions should be accompanied by illustrations for comprehensibility, similar to illustrative examples in the *Penal Code, 1860*. For instance, additional explanation to the definition of "digitally created pornography" could highlight that the definition specifically requires the content to depict the likeness of a real person, or that the depiction can be visual or audio representation of a real person, or that digital tools and technologies must be used to create the at-issue content, even if a basic raster graphics editor application is used to superimpose the face of a real person onto an explicit image of another person's body.

Revise the statute to reflect online consumption of pornography. Current framework does not explicitly refer to online production or distribution. Digital platforms, social media, live-streaming services, and algorithm-based content delivery are the primary channels of consumption of pornography, and should be specifically referenced either in the definitions or the scope and applicability sections of the law.

OFFENSES

Sections 4, 6, 8(7) — Criminalization of pornography, and search and seizure powers of LEA

ASSESSMENT

Arguably, while meeting the decency and morality grounds of restriction under the Constitution, the broad and absolute ban — encompassing production, storage, possession, marketing, transportation, supply, purchase, sale, or display of pornography, or abetment thereof under sections 4 and 8(7) — appears to exceed constitutional reasonableness standards. An undifferentiated ban on consensual adult content and unlawful forms of pornography, such as CSAM and TFSV, does not appear to be reasonable. A failure to differentiate between harmful and non-harmful content, and treating all sexually explicit materials as inherently damaging, also overlooks the need to address specific online harms. Moreover, many contemporary regulatory approaches increasingly distinguish between exploitative or abusive sexual content — such as CSAM, trafficking-related exploitation, non-consensual pornography, and coercive sexual abuse — and consensual adult pornography, recognizing that these categories engage fundamentally different harms and therefore warrant differentiated regulatory treatment. Absence of a nuanced regulatory framework that considers different types of content and contexts could render this provision constitutionally vulnerable to challenges, as well as overreaching and ineffective.

Specifically, criminalization of production, storage, and possession of consensual explicit materials for personal consumption or private, non-commercial uses constitutes a state overreach into private affairs that can be seen as a violation of the right to privacy and access to information, as well as personal freedom. Given the broad search and seizure mandate of LEA under section 6, and the allowance for seized device and data to be openly presented as evidence in court, this provision poses a significant threat to the confidentiality and autonomy of individuals, and creates risks of exposing private and intimate conduct between consenting

adults to public scrutiny, in addition to criminal liability — creating avenues for invasive state surveillance and punitive measures against individuals for personal or political reasons.

Furthermore, the abetment provision in section 8(7) — which attributes liability and punishment to individuals who are directly involved in or aiding and abetting of the offense — does not adequately distinguish between different levels of involvement or culpability, potentially leading to disproportionate punishments for those whose participation in the alleged offense was minimal, indirect, or innocent. Particularly, in the context of digitally recorded and stored content, where the line between passive and active involvement can be blurry, this provision could have far-reaching and unintended consequences. This approach runs counter to the principles of proportionality and fairness in criminal justice, which require that punishments correspond to the nature and gravity of the offense and the offender's level of culpability.

From a policy and implementation perspective, the provision fails to recognize the realities and dynamic nature surrounding pornography dissemination and consumption (and to a lesser extent, production) in Bangladesh. Contemporary pornography ecosystems are predominantly platform-mediated, transnational, encrypted, algorithmically distributed, and increasingly user-generated, including through subscription-based adult content services, live-streaming platforms, and interactive digital platforms. In this context, distribution of and access to pornography via the internet makes monitoring and enforcement not only difficult but also impractical, especially when much of the content is hosted on servers outside the jurisdiction of domestic law, and the statute does not have meaningful extraterritorial reach, thereby creating avenues for selective and arbitrary enforcement. Furthermore, the provision also risks overburdening law enforcement resources, diverting attention from more pressing issues such as combating CSAM, TFSV, human trafficking, and other forms of sexual exploitation. Earlier strategies of geo-blocking access to pornographic websites at the network level, reportedly in the tens of thousands, have been ineffective due to increasing awareness and use of proxies and encryption systems, such as virtual private networks, to bypass censorship measures.

RECOMMENDATIONS

Amend the broad and absolute ban on production, storage, possession, marketing, transportation, supply, purchase, sale, or display of pornography, and enhance enforcement capacity.

Introduce differentiated legal treatment for different types of content. Rather than criminalizing all adult content, shift enforcement priorities to target more pressing issues such as CSAM and TFSV. Amend sections 4 and 8(7) to expressly differentiate between non-harmful, consensual adult content and harmful pornography.

For instance, content depicting CSAM could be treated as a strict liability offense, with production, storage, possession, marketing, supply, purchase, sale, or display each a distinct offense of equal severity to address the broader policy objective of curbing child sexual offenses (*see*, for instance, the *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse* and the *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*). Conversely, the statute may impose greater restrictions and higher penalties on recording, creation, and/or dissemination of non-consensual or digitally created pornographies, introducing a lower threshold by including both intention and recklessness in consent to afford higher degree of protection (as Australia did through enactment of the *Criminal Code Amendment (Deepfake Sexual Material) Act 2024* to amend the *Criminal Code Act 1995*; *see also* the *Proposal for a Regulation of the European Parliament and of the Council on combating violence against women and domestic violence* addressing non-consensual sharing of intimate or manipulated material) but lower sanctions for their possession and consumption, recognizing that those involved in the production and distribution of such materials play a more active and harmful role, whereas individuals possessing or consuming it may

be less directly involved in its creation, and requires rehabilitation or education rather than severe punitive measures.

Any sexually explicit content involving consenting adults that is produced or distributed for private, non-commercial consumption, or for significant literary, research, artistic, political, cultural, historical, religious, educational, media reporting, criminal investigation, medical, or scientific value or purpose, should be decriminalized, to align with privacy rights and the freedom of personal expression. This will offer clearer guidelines and protections for content creators, publishers, and distributors to avoid legal uncertainty and ensure they can distinguish between lawful and unlawful material.

Adopt code of conduct and public education materials. Similar to the approaches adopted by the United Kingdom and Australia, in additional to primary legislations, adopt codes of conduct and disseminate public interest materials to combat harmful pornographic content (*see*, for instance, the *interim code of practice on online child sexual exploitation and abuse* and the *voluntary guidance for internet infrastructure providers on tackling online child sexual exploitation and abuse* in the United Kingdom, the *child protection guide for assessing, preventing and responding*, *adult cyber abuse scheme*, *image-based abuse scheme*, and *online content scheme*, as well as the materials on protecting children from sexual abuse online and child sexual abuse online in Australia). Such measures provide clear and consistent standards for technology companies, law enforcement, and governments to coordinate and work collaboratively, guiding them on how to detect, report, and remove harmful pornographic materials effectively, while also educating parents, children, and the broader community.

Redefine abetment and liability. Amend the abetment provisions in section 8(7) to distinguish between varying levels of culpability, ensuring that individuals with minimal or indirect involvement are not subjected to disproportionate punishments.

Enhancement of enforcement capacity. Existing measures, such as geo-blocking pornographic websites en masse, are ineffective due to increased use of censorship circumvention tools, like virtual private networks. Instead, other measures could be adopted. First, the penalty regime should be reformed to align with gravity of the offense and the offenders' culpability, avoiding over-criminalization of personal or private consumption of consensual adult content. Second, mechanisms should be adopted to enable cross-border cooperation to combat harmful content and enforcement, direct law enforcement resources towards combating high-priority cybercrimes, and develop specialized units focused on addressing severe forms of online sexual exploitation, rather than over-policing adult consensual content. Finally, there should be clear safe harbor provision and notice-and-takedown regime so that while intermediaries are protected from liability for third-party user-generated content, they can be held liable for failure to remove or disable access to illegal content upon receiving notice, ensuring a balance between preventing the dissemination of harmful material and safeguarding free expression and innovation in the digital ecosystem.

Section 10 — Cognizability and non-bailability of offenses

ASSESSMENT

Cognizability and non-bailability of offenses under the statute means an investigating officer can arrest accused without a warrant and initiate investigation without prior judicial approval, and bail is not a matter of right and is subject to judicial discretion. Given the vague definition of "pornography" and over-criminalization, it may lead to police overreach and abuse in situations that do not warrant such severe measures, including unnecessary detention and prolonged legal battles, and judicial persecution considering broad discretion in denying bail. Applying cognizability and non-bailability to offenses

under these provisions undermines constitutional protections of presumption of innocence, protection from arbitrary detention, and the right to a fair trial. It also runs counter to the policy intent behind these classifications, aimed to address serious and high-priority crimes effectively by diverting resources away from more less serious crimes and focusing on critical areas of intervention.

RECOMMENDATIONS

Amend the cognizability and non-bailability of offenses.

Reclassify offenses. Amend the statute to decriminalize the majority of offenses related to consensual adult content. Relatively minor offenses and criminal behavior, such as public indecency, or content featuring extreme acts, should be non-cognizable and bailable, limiting arrest powers of law enforcement without a warrant and enabling judicial oversight before initiating an investigation. Adjust penalties to reflect the seriousness of the offense, ensuring minor offenses related to consensual content are met only with civil penalties, warnings, or fines, rather than criminal prosecution and incarceration. On the other hand, content depicting CSAM, TFSV, bestiality, human trafficking, and other severe forms of sexual exploitation, could be cognizable and non-bailable, with clear guidelines for courts to follow when assessing bail applications.

Section 8 — Criminal penalties for up to ten years' imprisonment and BDT 500,000 fine

ASSESSMENT

While the penalty regime is graded — imposing lower punishment for adult sexual materials and higher punishment for child pornography — it is not sufficiently nuanced to proportionally address the varying severity of offenses. For example, it does not distinguish between consensual adult content and exploitative or harmful material; the same punishment of rigorous imprisonment ranging from seven to ten years and fines of up to BDT 500,000 may apply to both the production of pornography and the coercion of individuals, including children, into participating, despite the vastly different degrees of harm involved. At the same time, certain offenses such as revenge porn and CSAM are separately criminalized under section 25 of the *Cyber Protection Act, 2026* with substantially different penalty regimes — including imprisonment of up to two years and fines of up to BDT 10,000,000, increasing to five years' imprisonment and BDT 20,000,000 where offenses are committed against women and children. This creates inconsistency in legislative design and raises concerns regarding proportionality, coherent sentencing policy, and arbitrary prosecutorial discretion. Over-criminalization may erode respect for the legal system, contribute to widespread non-compliance and underreporting, and risk driving harmful activities further underground. Overall, the penalty regime is disproportionate and appears to contravene the rights to free speech, equality before the law, and due process guarantees enshrined in constitutional and international human rights frameworks. Added to that, the vagueness and subjectivity of these offenses, coupled with their non-bailable and cognizable nature, further exacerbate the potential for abuse.

Absent sentencing guidelines, a recommendation system, or a central database for cases decided across the country, judges are left with broad discretion, undermining the fairness and consistency of the sentencing process. In turn, this can potentially result in an arbitrary, disproportionate, and fragmented penalty regime, systemic biases and inequalities in sentencing, and failure to achieve broader social goals such as deterrence and rehabilitation, infringing equal protection and legal certainty principles and citizens' right to a fair trial, and undermining public confidence in the judiciary and the rule of law.

RECOMMENDATIONS

Amend the criminal sanctions provision.

Introduce a tiered penalty system. Differentiate penalties based on the type and severity of offenses, with lighter punishments for consensual adult content (e.g., short prison sentence, civil or criminal fines, or warnings) and stricter penalties for exploitative or harmful material (e.g., CSAM and TFSV), consistent with proportionality principles. As recommended above, pornography should be differentiated, and penalized differently, from more serious offenses — each carrying penalties and enforcement priorities proportional to the seriousness of the harm. Additionally, exclude consensual adult content for personal use from criminal sanctions, while retaining strict, tiered penalties for commercial exploitation, distribution, or content that involves harm or coercion.

Introduce sentencing guidelines and centralized case tracking system. A blanket punishment of maximum seven years' imprisonment for all forms of pornography related offenses, without any sentencing guidelines, attracts arbitrary sentencing. Establish clear sentencing guidelines addressing different offenses to ensure uniformity and proportionality in the application of penalties, limit judicial discretion, and avoid arbitrary sentencing. Clarification on how sentencing discretion should be exercised when dealing with multiple offenses — such as deepfake pornography overlapping with CSAM or non-consensual pornography — should be clearly articulated in the guidelines. Illustratively, the sentencing guidelines should state whether, and under what circumstances, should an accused be sentenced concurrently and consecutively, and what the maximum punishment should be in the event of consecutive term. Furthermore, introduce a centralized system for tracking case precedents, allowing courts to consult a database to ensure consistent sentencing across the judiciary.

7. Competition Act, 2012

The *Competition Act, 2012* reflects a predominantly traditional approach to market regulation that is increasingly insufficient to address the realities of contemporary digital markets and platform ecosystems. The assessment identifies several structural limitations across the framework, including narrow and price-centric definitions of "relevant market" and "service," inadequate recognition of data-driven and attention-based business models, and insufficient guidance regarding technologically mediated forms of anti-competitive conduct within digital ecosystems. As currently framed, the statute does not adequately account for factors such as network effects, data concentration, ecosystem integration, interoperability restrictions, algorithmic curation, ecosystem lock-in, self-preferencing, exploitative click-through agreements, anti-steering restrictions, exclusionary data practices, and cross-market leveraging that increasingly shape market power and competition in digital platform economies. While certain provisions may be broad enough in principle to capture some forms of digital market abuse, the framework lacks the conceptual clarity, technical specialization, institutional capacity, and explicit extraterritorial mechanisms necessary to consistently regulate increasingly complex cross-border digital ecosystems and offshore digital platforms operating within Bangladesh. Comparative developments across jurisdictions increasingly recognize the need for technologically adaptive, data-centric, and ecosystem-aware approaches to digital competition regulation.

Accordingly, the overall recommendation is substantial modernization of the statute through a technologically contemporary and platform-aware competition framework capable of addressing the realities of digital markets. The statute should modernize relevant definitions, introduce clearer digital-specific standards for abuse of dominance and anti-competitive conduct, expressly regulate platform-mediated harms and exclusionary digital practices, and clarify extraterritorial applicability to offshore digital entities. We further recommend strengthening institutional capacity through specialized digital market expertise within the Competition Commission, enhanced technical advisory mechanisms, and authority to issue issue-specific guidelines and codes of practice capable of adapting to rapidly evolving digital ecosystems without requiring frequent legislative amendment.

SCOPE AND APPLICATION

Sections 3, 22 — Application of the law

ASSESSMENT

While the statute applies to all enterprises involved in the provision of "services for commercial purposes" and section 22 confers the Competition Commission the authority to enquire into any conduct outside the country that has adverse impact on the relevant market, it lacks explicit extraterritorial provisions. Although there is a general presumption against extraterritoriality of statutes, comparative jurisprudence increasingly demonstrates that courts and regulators may adopt effects-based or recipient-location approaches to extend domestic regulatory obligations to offshore digital entities whose services substantially affect local consumers or markets. For instance, in India, competition authorities and courts have interpreted a similar provision, section 32 of the *Competition Act, 2002*, to permit assertion of jurisdiction over global platform conduct producing anti-competitive effects within domestic digital markets, notwithstanding

offshore corporate structures and cross-border digital service delivery (*see* *Google LLC v Competition Commission of India*). However, comparative experience also demonstrates that even where statutes expressly provide for extraterritorial application, practical enforcement against overseas digital platforms remains legally and operationally complex, particularly in relation to cross-border compliance, intermediary resistance, conflicting jurisdictional claims, and enforceability of domestic orders abroad — this was illustrated by the Australian regulator's unsuccessful attempt to operationalize a global removal order against X (*see* *eSafety Commissioner v X Corp*). Nevertheless, legal certainty and due process principles, and risks associated with inconsistent and unpredictable enforcement against offshore companies leading to jurisdictional disputes, warrant amendment to the provision to expressly mandate extraterritorial application.

RECOMMENDATIONS

Amend and incorporate extraterritoriality provision and enforcement mechanisms.

Incorporate explicit extraterritoriality provisions. Amend the statute to clearly define its extraterritorial reach, explicitly stating that it applies to offshore companies providing services to users in Bangladesh, ensuring it covers cross-border digital services and transactions (*see*, for instance, Article 1(2) of the EU's *Digital Markets Act* and Article 3 of GDPR). Establish clear criteria based on the location of the service recipient, data flows, or market impact, ensuring that companies outside Bangladesh are subject to the statute when their services significantly affect the local market. Ensure that the statute includes safeguards for foreign companies, such as the right to fair hearings, notification, and appeal processes, to prevent jurisdictional overreach and align with international legal standards.

Clarify enforcement mechanisms for offshore entities. Specify the legal procedures for enforcing the statute against foreign entities, including how penalties, investigations, and legal actions can be carried out on offshore companies providing services to Bangladeshi users. Specifically, introduce provisions for cooperation between the Competition Commission and international regulatory bodies to facilitate enforcement against foreign companies and resolve cross-border jurisdictional disputes effectively (*see* the *International Antitrust Enforcement Assistance Act of 1994* and the *Antitrust Guidelines for International Enforcement and Cooperation* in the United States and Part III of the *Competition Act 1985* of Canada).

Antitrust enforcers worldwide have entered into agreements for cross-border enforcement (*see*, for example, agreements between the United States and Australia and Japan and India, multi-agency agreements between Australia, Canada, New Zealand, the United Kingdom, and the United States and Brazil, China, India, Russia, and South Africa, and agreements entered between European Commission and countries outside of the European Union). Bangladesh could similarly enter into a multi-country agreement for more effective enforcement.

DEFINITIONS

Section 2(s) — Definition of "relevant market"

ASSESSMENT

As currently defined, the term focuses on the exchangeability and substitutability of goods or services based on characteristics, price, and intended use, as well as the homogeneity of competition conditions within a specific geographic area — this is insufficiently nuanced to adequately address the unique dynamics of digital markets. Particularly in the context of e-commerce and social media services that operate on a cross-border basis, markets can be national, regional, or global, and the competition dynamics in one country can be influenced by actions taken in another. A geographically confined and price-centric definition of markets therefore fails to adequately account for the transnational and multi-sided nature of digital platforms, potentially resulting in inaccurate assessments of dominance, anti-competitive conduct, and market power.

The framework also reflects an outdated understanding of online market dynamics, where factors beyond price and product characteristics — including control over data, network effects, switching costs, interoperability limitations, attention capture, algorithmic curation, lock-in effects, economies of scale, and platform ecosystem integration — increasingly shape consumer behaviour and competitive advantage, particularly in markets for social media, search, e-commerce, and digital advertising. For example, a social media platform's market power is often derived less from price or product characteristics than from its user base, data collection and combination capabilities, advertising infrastructure, and ability to leverage network effects to entrench market dominance and outcompete rivals. Failure to incorporate these considerations into the definition of relevant market may result in ineffective or distorted competition analysis, either by underestimating anti-competitive conduct in digital ecosystems or by misidentifying market power and competitive constraints. Furthermore, competition in digital markets is rarely homogeneous, even within a single country, due to varying levels of internet penetration, digital literacy, infrastructure access, linguistic diversity, payment systems, and local consumer preferences.

RECOMMENDATIONS

Amend the definition.

Expand and modernize the definition of "relevant market". Amend the definition of "relevant market" to account for the global nature of digital platforms and services, ensuring cross-border competition and actions affecting other jurisdictions are included in assessments. Specifically, the definition should be modified to encompass factors beyond traditional market attributes like price and product characteristics — such as user base, data capabilities, network effects, and platform economics, which are pivotal to digital competition, especially in sectors like social media and online advertising. The framework should also remain sufficiently flexible to account for heterogeneous and evolving digital market conditions, including variations in internet penetration, infrastructure access, digital literacy, payment systems, linguistic diversity, and local consumer behaviour, thereby enabling more context-sensitive and dynamic assessments of competition and market power.

The definition should further expressly recognize the possibility of cross-market leveraging and anti-competitive conduct across interconnected digital ecosystems and multiple related markets. For instance,

the Competition Commission of India imposed a fine of Rs. 1337.76 crore against Google in 2022 for engaging in anti-competitive practices across multiple markets for operating systems, mobile application stores, general web search services, non-operating system specific mobile web browsers, and online video hosting platform within India (*see* press release by Competition Commission of India).

Comparative frameworks increasingly recognize these dynamics. For example, the European Commission's *Commission Notice on the Definition of Relevant Market for the Purposes of Union Competition Law 2024* expressly acknowledges multi-sided platforms, digital ecosystems, network effects, zero-price services, attention markets, and data-driven market power within relevant market assessments. Similarly, section 18(3a) of the German *Competition Act 2013* specifically requires consideration of factors such as direct and indirect network effects, switching costs, economies of scale, access to competitively relevant data, innovation-driven competitive pressure, and the intermediary power of digital platforms when assessing market dominance in digital markets.

Section 2(t) — Definition of "service"

ASSESSMENT

While the definition covers "service of any description" and includes those related to industrial or commercial matters,it remains insufficiently tailored to the realities and unique characteristics of contemporary digital services and platform ecosystems. Online intermediaries — including social media, streaming services, search engines, app stores, and digital marketplaces — provide services without direct monetary payment from users, instead relying on user data, user attention, behavioural profiling, and advertising-driven monetization models, where the value exchange in digital transactions does not align neatly with traditional commercial models. Absent a clearer and more technologically contemporary legal framework, this creates risks of both regulatory gaps and overreach, potentially resulting in inconsistent application and uncertainty regarding the scope of regulation.

Furthermore, these platforms operate on a data-driven business model that rely on cross-side, multi-side, and same-side network effects, where the value of the service increases with the number of users on different sides of the platform (e.g., advertisers and consumers). The current definition therefore provides insufficient guidance regarding when and how digital services — particularly zero-price or attention-based services — fall within the scope of regulation, especially where no direct financial consideration is exchanged between users and service providers.

RECOMMENDATIONS

Amend the definition.

Expand and modernize the definition of "service". Amend the definition of "service" to include data- and attention-based models that are not reliant on direct financial remuneration, where data and attention are the key value drivers and currency of exchange, thus capturing modern online intermediaries and platforms (*see* Article 2 of the EU's *Digital Markets Act*). The statute should also establish clearer and more objective thresholds for determining when a digital service becomes subject to regulation, including in circumstances where services are provided without direct monetary consideration, in order to improve legal certainty and regulatory predictability for platforms and intermediaries.

For greater conceptual clarity, the definition and overall framework should further recognize the operation of cross-side, same-side, and multi-sided

platform business models — such as social media platforms, app stores, search engines, e-commerce marketplaces, and digital advertising ecosystems — where value is generated through interactions among multiple categories of users, advertisers, merchants, developers, and content creators, and where market dynamics differ fundamentally from traditional one-sided commercial markets (*see* European Commission's *Commission Notice on the Definition of Relevant Market for the Purposes of Union Competition Law 2024* and the German *Competition Act 2013* referenced above). The framework should therefore expressly acknowledge factors such as network effects, ecosystem integration, switching costs, interoperability limitations, and data concentration when assessing the scope and nature of regulated digital services.

ANTI-COMPETITIVE BEHAVIOR

Sections 15, 16 — Anti-competitive agreement, and abuse of dominant position

ASSESSMENT

Although well-intentioned to encourage fair competition, these provisions are not sufficiently nuanced to address the realities of the modern digital ecosystem. The existing definitions do not adequately capture the multifaceted nature of the digital marketplace, where many service providers operate multi-sided and cross-sided platforms, facilitating interactions between users, advertisers, and content creators in a manner that does not neatly fit into definitions of "relevant market" or "service," nor do they align with conventional competition metrics such as price and market share. In digital markets, where business practices often deviate from traditional norms — such as offering services for "free" in exchange for user data and attention, rather than direct financial remuneration — the provisions risk being either over-inclusive or under-inclusive. As a result, certain digital platforms may be wrongly classified as anti-competitive, while others may evade appropriate scrutiny despite exercising substantial market power.

The framework also provides insufficient guidance regarding what constitutes "abuse of dominant position" or "anti-competitive behaviour" within digital ecosystems. For instance, pricing strategies essential for digital platforms to scale and compete globally might be misinterpreted as predatory under the current legal framework, simply because they involve offering services at a low or no cost to users. Overly rigid interpretation may therefore risk stifling innovation, discouraging market entry, and failing to accurately assess consumer harm and competitive effects in data-driven markets.

For instance, the statute's focus on traditional price-based anti-competitive behavior in section 15, such as on agreements that impact goods or services through price-fixing, bid rigging, or supply restrictions, does not capture the non-monetary value exchange central to the digital economy. Digital platforms such as Alphabet and Meta frequently provide ostensibly "free" services while monetizing extensive user data collection, behavioral profiling, advertising infrastructure, and ecosystem integration. A failure to recognize data and user attention as sources of market power may therefore allow anti-competitive conduct to escape effective scrutiny despite substantial dominance within digital ecosystems. Illustratively, the provisions fail to adequately address click-through and bundled user agreements commonly used by digital platforms to condition access to services on extensive data-sharing, ecosystem integration, or acceptance of unrelated contractual obligations that may restrict interoperability, limit switching, or foreclose competition. For example, the German Federal Cartel Office found, and the Court of Justice of the European Union agreed, that Meta abused its dominant position by conditioning use of Facebook on extensive cross-platform data collection and combination practices, thereby reinforcing its market power through click-through agreement in digital

advertising and social networking markets.

Certain provisions related to abuse of dominant positions, specifically section 16(2)(c), (d), and (e), may be broad enough in their language to encompass a wide range of activities by, for instance, FAANG+ companies. At least in theory, these may include restricting market access through restrictive data practices, self-preferencing, interoperability restrictions, tying and bundling practices, conditioning access to services on extensive personal data access, or leveraging dominance in one market to gain competitive advantages in adjacent or downstream markets. For instance, Google could leverage dominance in search markets to preference affiliated services, while Amazon could use third-party seller data to advantage its own products and services. However, despite this breadth, the framework remains insufficiently calibrated to address the structural realities of digital competition, where network effects, algorithmic curation, data concentration, ecosystem integration, interoperability limitations, and platform "walled gardens" may significantly distort consumer choice and competitive conditions in ways not adequately captured by traditional competition analysis.

RECOMMENDATIONS

Amend and redefine the remit of anti-competitive behavior to accommodate harms in the digital markets.

Set clearer digital market thresholds for abuse of dominance and anti-competitive conduct. Redefine the threshold for what constitutes anti-competitive behavior in digital markets, moving beyond pricing strategies to include data practices, network effects, and the ability to leverage dominance in one market to influence another. Comparative frameworks such as section 18(3a) of the German *Competition Act 2013*, Article 5-7 of the EU's *Digital Markets Act*, and the United Kingdom's *Digital Markets, Competition and Consumers Act 2024* increasingly recognize factors including direct and indirect network effects, access to competitively relevant data, economies of scale, innovation-driven competitive pressure, interoperability restrictions, ecosystem integration, and intermediary power in digital market assessments. The framework should therefore adopt data-centric competition metrics that assess the scale, sensitivity, portability, combination, and strategic use of collected data when evaluating market dominance and anti-competitive effects.

Equally important is to clarify that digital platform business models involving zero-price or low-cost services, cross-subsidization, introductory pricing, or advertising-funded services should not automatically be treated as predatory or anti-competitive absent demonstrable exclusionary effects or consumer harm (*see* reports by the United States House Judiciary Committee's Investigation of Competition in Digital Markets, and by the Australian Competition & Consumer Commission on Digital Platforms Inquiry and Digital Platform Services Inquiry, as well as interim reports on social media services, mobile applications services and marketplace, web browsers and general search services and choice screens, general online retail marketplaces, and data products and services; *see also* Japan's *Mobile Software Competition Act 2024* and the *Mobile Software Competition Act Guidelines 2025*, which recognizes that certain app store and mobile ecosystem practices may require ex ante regulation while also preserving objective justifications relating to cybersecurity, privacy, and system integrity).

Expand and modernize the scope of anti-competitive behavior in digital markets. Identify and incorporate new categories of anti-competitive behavior. Certain exclusionary and anti-competitive practices commonly associated with dominant digital platforms should be expressly recognized within the statute, including:

(a) systemic monopolistic conduct and self-preferencing behavior; for instance, Alphabet leveraging dominance in search and advertising technology markets to preference affiliated services such as shopping, cloud, streaming, or other vertically integrated services (*see United States v. Google LLC* (2020) and *United States v. Google LLC*

(2023), and the investigation report of the United States House Judiciary Committee's Investigation of Competition in Digital Markets (2020); and section 19a of the German *Competition Act 2013* and *Alphabet Inc. v. Germany* in Germany).

(b) abuse of dominant position in mobile application distribution and app store ecosystems; for instance, Apple and Alphabet compelling developers to use proprietary payment gateways, restricting alternative payment systems, and imposing anti-steering and interoperability limitations (*see Epic Games v. Google* in Australia; *Epic Games v. Apple* and *Epic Games v. Google* in the United States, where a permanent injunction was issued against Apple and Google; see also press release by the Competition Commission of India imposing a monetary penalty of Rs. 936.44 crore on Google, and the investigation against Apple in India; comparable concerns are also reflected in Japan's *Mobile Software Competition Act 2024* and South Korea's *Telecommunications Business Act*).

(c) abuse of dominance in e-commerce and marketplace ecosystems; for instance, Amazon engaging in exclusionary conduct through use of third-party seller data, self-preferencing, discriminatory ranking practices, algorithmic manipulation, and marketplace practices that distort fair competition (*see Federal Trade Commission v. Amazon.com, Inc.* and *State of Arizona v. Amazon.com, Inc.* in the United States; the statement of objections issued by European Commission and the commitments by Amazon to address competition concerns over its use of non-public marketplace seller data and over a possible bias in granting sellers access to exclusive features in the European Union; similar commitments were accepted by the Competition and Markets Authority in the United Kingdom; these concerns are also increasingly addressed under the interoperability and conduct requirements contained in the EU's *Digital Markets Act* and the United Kingdom's *Digital Markets, Competition and Consumers Act 2024*).

(d) exclusionary ecosystem design and interoperability restrictions; for instance, Apple limiting interoperability for third-party digital wallets, smartwatches, messaging applications, and related services within its ecosystem (*see United States v. Apple Inc.*).

(e) collusive or exclusionary default arrangements; for instance, Apple, Google, device manufacturers, and carriers entering into exclusive arrangements establishing Google as the default search engine across browsers and devices, thereby reinforcing search dominance and limiting market access for competitors (*United States v. Google LLC* in the United States; *see also* Digital Platform Services Inquiry – September 2024 report revisiting general search services in Australia).

(f) abusive acquisition strategies, exclusionary data practices, algorithmic self-preferencing, and cross-market leveraging of user data to entrench ecosystem dominance and eliminate nascent or potential competitors; for instance, Meta engaging in such conduct through ecosystem integration and data-combination practices (*see* the settlement order between Meta and the Federal Trade Commission for US$ 5,000,000,000 in the United States, and the Digital Platform Services Inquiry, Interim Report 7 in Australia; *see also* press release by the Competition Commission of India imposing a Rs. 213.14 crore against Meta for anti-competitive practices in relation to its privacy policy update).

Additionally, the statute should expressly prohibit exploitative tying and bundling practices, restrictive click-through and consent-based contractual arrangements, anti-competitive interoperability restrictions, abusive cross-market leveraging of data or market power, exploitative default settings and choice architecture, and the creation of "walled gardens" through data monopolization, ecosystem lock-in, and switching barriers that undermine consumer choice and fair competition.

Regulate anti-competitive click-through and consent-based agreements. Amend the statute to address anti-competitive click-through agreements, where users are mandatorily required to accept terms that grant excessive access to personal data or restrict access to competing services. Comparative jurisprudence such as

Meta v. Bundeskartellamt, proceedings involving Google and Meta before the German Federal Cartel Office, and the *Douglas Italia* decision increasingly recognize that coercive consent bundling, excessive data access conditions, and integrated click-through agreements may constitute anti-competitive and exploitative conduct within digital platform ecosystems.

INSTITUTIONAL STRUCTURE

Section 7(1), 7(3) — Composition of the Competition Commission

ASSESSMENT

This provision fails to adequately account for the highly technical and specialized nature of digital markets, potentially limiting the Competition Commission's effectiveness in regulating competition within complex digital ecosystems. The current qualification framework — framed broadly around experience in economics, market affairs, public administration, or law — does not ensure that members of the Competition Commission possess the specialized expertise necessary to understand and assess digital market dynamics, including algorithms, platform economics, artificial intelligence systems, interoperability restrictions, data-driven business models, network effects, digital advertising ecosystems, and the rapid pace of technological change. Without such expertise, the Competition Commission risks becoming an insufficiently calibrated regulatory body, unable to effectively distinguish between legitimate competitive innovation and genuinely anti-competitive conduct in digital markets. In practice, this may result either in over-regulation that stifles innovation and market entry, or under-regulation that permits exclusionary conduct, ecosystem lock-in, and concentration of market power by dominant digital platforms to persist without effective oversight.

RECOMMENDATIONS

Amend the organizational structure of the Competition Commission.

Mandate specialized digital market expertise within the Competition Commission. Amend the statute to require that a certain number of members of the Competition Commission have specific expertise in digital markets, including areas like algorithms, data-driven business models, and digital platform economics. This may be operationalized through the establishment of a dedicated digital markets or technology competition unit within the Competition Commission tasked specifically with digital competition and platform governance matters and staffed with technical, economic, and legal experts. Additionally, the statute should expressly empower the Competition Commission and its specialized unit to consult independent external experts in data science, software engineering, artificial intelligence, cybersecurity, digital infrastructure, and related technical disciplines when assessing anti-competitive conduct within digital ecosystems.

The statute should further require periodic and continuing capacity-building and training for members and staff of the Competition Commission on emerging technologies, digital business models, artificial intelligence systems, data governance, platform economics, and evolving international regulatory approaches to digital competition. Furthermore, the framework should establish formal mechanisms for structured engagement and regular dialogue between the Competition Commission and relevant stakeholders, including technology companies, consumer groups, civil society organizations, academics, technical experts,

and foreign regulators and competition authorities. Such engagement would support more informed, transparent, and technically grounded decision-making while facilitating regulatory cooperation and development of context-sensitive digital market policies.

Finally, the statute should expressly authorize the Competition Commission to issue issue-specific rules, codes of practice, guidelines, and advisory frameworks relating to digital market conduct, including matters such as self-preferencing, interoperability, algorithmic transparency, network effects, ecosystem integration, data concentration, app store restrictions, and platform lock-in strategies, without requiring frequent legislative amendment. These reforms would help ensure that the Competition Commission possesses the institutional capacity, technical expertise, and regulatory flexibility necessary to effectively oversee increasingly complex and rapidly evolving digital ecosystems.

8. Consumer Rights Protection Act, 2009

The *Consumer Rights Protection Act, 2009* reflects a predominantly traditional and transaction-centric understanding of commerce that is increasingly inadequate for regulating contemporary digital markets and platform ecosystems. The assessment identifies several structural limitations across the framework, including narrow and outdated definitions of "consumer," "service," and "anti-consumer right practice," inadequate recognition of data-driven and attention-based business models, and the absence of meaningful safeguards against digitally mediated consumer harms. As currently framed, the statute does not sufficiently address harms arising from algorithmic manipulation, dark patterns, exploitative data practices, personalized pricing, recommender systems, platform dependency, and opaque advertising and profiling systems increasingly deployed by large digital platforms. The framework also lacks explicit extraterritorial applicability, creating uncertainty regarding enforcement against offshore digital platforms and cross-border online services operating within Bangladesh.

Accordingly, the overall recommendation is substantial modernization of the statute through a technologically contemporary and platform-aware consumer protection framework capable of addressing the realities of the digital economy. The statute should modernize and expand key definitions, recognize data and attention as forms of consideration, expressly regulate digitally mediated consumer harms and manipulative platform practices, and clarify applicability to offshore digital service providers operating cross-border services in Bangladesh. We further recommend empowering the DNCRP to issue issue-specific rules, codes of practice, and advisory guidelines relating to emerging digital harms, while strengthening protections against exploitative data practices, algorithmic manipulation, dark patterns, and AI-enabled consumer harms in line with evolving international approaches to digital consumer protection.

SCOPE AND APPLICATION

Section 1 — Application of the law

ASSESSMENT

The statute does not clearly define its territorial scope or expressly address extraterritorial application. As currently framed, while the statute would apply to enterprises operating within Bangladesh, it remains unclear whether its provisions are enforceable against offshore entities providing goods or services to consumers in Bangladesh on a cross-border digital basis. In practice, this creates legal uncertainty regarding the applicability of consumer protection obligations to foreign e-commerce platforms, digital intermediaries, app-based services, and other overseas digital service providers increasingly active in the domestic market. The absence of explicit extraterritorial provisions may therefore create regulatory gaps and enforcement limitations in relation to cross-border digital transactions and platform-based consumer harms.

RECOMMENDATIONS

Amend the scope and application.

Expressly provide for extraterritorial applicability in relation to cross-border digital services. Amend the statute to ensure it applies to offshore companies providing digital services to users in Bangladesh, even if the company does not have a physical presence in the country (*see* section 3 of New Zealand's *Fair Trading Act 1986* and section 5(8) of South African *Consumer Protection Act, 2008*; *see also*, for instance, Article 1(2) of the EU's *Digital Markets Act* and Article 3 of the GDPR, as well as emerging platform regulation frameworks in jurisdictions such as Australia and India that increasingly adopt effects-based or user-location approaches to digital regulation). Such reform would help ensure that large transnational digital platforms and offshore service providers offering cross-border digital services to consumers in Bangladesh remain subject to meaningful consumer protection obligations and regulatory oversight. To avoid disproportionate or overly broad application, the statute should establish clear jurisdictional thresholds and nexus criteria, such as the scale of commercial activity directed toward Bangladesh, user base size, revenue generated from Bangladeshi users, targeted advertising, localized platform operations, or systematic offering of goods or services to persons within Bangladesh (*see* Article 3 of the EU's *Digital Markets Act* and section 1798.140(d) of the *California Consumer Privacy Act of 2018*, as well as the United Kingdom's Strategic Market Status framework under the *Digital Markets, Competition and Consumers Act 2024*).

DEFINITIONS AND ANTI-CONSUMER RIGHT SERVICES

Sections 2(19), 2(3), 21 — Definitions of "consumer" and "complainant," authority of DG-DNCRP

ASSESSMENT

From a legal and definitional perspective, the traditional conceptualisation of a "consumer" as purchasers of goods or services for consideration does not align with the realities of digital markets where user data and attention being the primary currency rather than direct financial remuneration. Although the existing definition may adequately apply to conventional e-commerce platforms such as Daraz or Foodpanda, it does not sufficiently capture the nature of digital transactions involving social media platforms, search engines, app stores, streaming services, and other ostensibly "free" online services, where users exchange personal data, behavioural information, content, and attention for access to digital platforms and services. This data-driven and attention-based techno-commercial model differs fundamentally from the conventional consumer transactions contemplated by the current statutory framework. Failure to recognize data and attention as forms of consideration may create significant regulatory gaps relating to privacy, profiling, algorithmic manipulation, targeted advertising, and exploitative platform practices, leaving consumers vulnerable to forms of harm not adequately addressed through traditional consumer protection concepts or remedies.

Furthermore, the definitions contained in sections 2(3) and 2(19) are not sufficiently future-proofed or technologically adaptive to regulate increasingly complex digital ecosystems in which consumers, advertisers, platforms, merchants, content creators, and intermediaries interact through multi-sided and data-driven business models. As a result, significant categories of consumer harms arising within the digital economy risk falling outside the effective scope of protection contemplated under the statute.

Moreover, the mandate of the DG-DNCRP under section 21, together with the broader architecture of

the legislation, reflects a predominantly traditional and transaction-centric understanding of commerce, where consumer protection is primarily concerned with the quality and safety of physical goods, pricing irregularities, misleading advertisements, and integrity of conventional commercial transactions. However, contemporary digital consumer harms increasingly arise not only from defective goods or deceptive transactions, but also from exploitative data practices, dark patterns, algorithmic bias, manipulative recommendation systems, platform dependency, unfair contractual terms, targeted advertising, addictive design practices, and anti-competitive platform conduct — issues that remain largely unaddressed within the current statutory framework.

RECOMMENDATIONS

Amend the definition and regulatory mandate.

Expand and modernize the definition of "consumer" and the scope of digital consumer harm. Redefine "consumer" to encompass individuals who provide personal data or attention as a form of non-monetary consideration in exchange for access to digital services. **Such reform would recognize users of ostensibly "free" digital services — including social media platforms, search engines, app stores, streaming services, and digital marketplaces — as consumers entitled to meaningful legal protection notwithstanding the absence of direct monetary payment.** Alternatively, the statute may adopt a technologically neutral and platform-agnostic definition of "consumer" that does not depend exclusively on monetary consideration or conventional transactional relationships (*see*, for instance, Article 3(c) of the EU's *Digital Services Act*).

Concurrently, the statute should be amended to introduce explicit protections against data exploitation and digitally mediated consumer harms, including unauthorized or excessive data collection, secondary data use, manipulative profiling, exploitative targeted advertising, dark patterns, algorithmic discrimination, addictive or manipulative interface design, opaque recommender systems, predatory data practices, and automated decision-making systems that adversely affect consumers (*see* Articles 5 and 6 of the EU's *Digital Markets Act*, Articles 34 and 35 of the *Digital Services Act*, and Articles 5 and 22 of the GDPR; *see* also the draft automated decision making technology regulations in the United States). Such reforms would help ensure that users of digital services receive meaningful protection against opaque and exploitative platform practices and have access to effective remedies in cases involving privacy violations, algorithmic harms, manipulative digital design, or misuse of personal data.

Section 2(22) — Definition of "service"

ASSESSMENT

The current definition of "service" is overly narrow, sector-specific, and prescriptive, primarily oriented toward traditional utilities and industries such as transport, telecommunications, healthcare, and similar conventional commercial sectors, while expressly excluding services provided without direct financial consideration. As a result, the definition fails to adequately capture the realities of the contemporary digital economy, where many of the most pervasive digital services — including social media platforms, search engines, app stores, streaming services, cloud services, and other online intermediaries — are provided without direct monetary payment and instead rely on user data, behavioral profiling, targeted advertising, and user attention as the principal mechanisms of value exchange.

By conditioning the definition of "service" on direct

financial remuneration, the statute leaves significant segments of the digital economy outside the effective scope of consumer protection regulation and fails to provide an adequate legal framework to address harms arising from digital platform ecosystems. The current framework also insufficiently addresses broader forms of digital consumer harm, including exploitative data practices, opaque profiling and recommendation systems, manipulative interface design, algorithmic bias, platform dependency, targeted advertising practices, and the growing influence of digital platforms over consumer behavior, public discourse, and information ecosystems.

The existing threshold for determining what constitutes a "service," tied narrowly to direct financial consideration, therefore reflects an increasingly outdated conception of commerce that does not adequately account for data-driven, attention-based, and platform-mediated digital business models.

RECOMMENDATIONS

Amend the definition.

Expand and modernize the definition of "service." Broaden the definition of "service" to expressly include non-remunerated, data-driven, attention-based, and platform-mediated services characteristic of the contemporary digital economy, where users provide personal data, behavioural information, content, or user attention in exchange for access to digital platforms and functionalities. The definition should therefore not be conditioned exclusively on direct monetary consideration or traditional transactional models. Specifically and explicitly include digital services such as social media platforms, search engines, app stores, online marketplaces, streaming services, cloud computing services, online advertising services, AI-enabled services, video-sharing platforms, digital payment systems, and other online intermediary services that significantly shape users' rights, behaviour, economic choices, and access to information (*see*, for instance, Article 2(c) of the *Unfair Commercial Practices Directive*, which includes goods and services, including digital service and digital content, as well as rights and obligations, in the definition of "product"; *see also* definitions of "core platform service," "information society service," "online social networking service," "video-sharing platform service," "cloud computing service," and "payment service" in the EU's *Digital Markets Act*). Such reform would help ensure that providers of ostensibly "free" digital services remain subject to meaningful consumer protection obligations and regulatory oversight proportionate to their influence over users, markets, data ecosystems, and digital public discourse.

Sections 2(20), 44, 45 — Definition of "anti-consumer right practice" and punishments

ASSESSMENT

Coupled with the restrictive definition of "service," the narrow, prescriptive, and transaction-centric definition of "anti-consumer right practice" under section 2(20) fails to adequately address the diverse, technologically mediated, and increasingly sophisticated forms of consumer harm arising within contemporary digital marketplaces and platform ecosystems. Furthermore, the framework remains heavily oriented toward traditional consumer harms relating to defective goods, misleading advertisements, pricing irregularities, or failure to provide services under sections 2(20)(d), 2(20)(e), 44, and 45. While these protections remain important, they are rooted in conventional and one-dimensional notions of commerce and do not sufficiently capture the realities and complexities of digital transactions, platform-mediated interactions, and data-driven business models.

For example, consumers within digital marketplaces may increasingly encounter harms arising from algorithmic ranking and recommendation systems, manipulative search prioritization, personalized or discriminatory pricing practices, exploitative click-through agreements, deceptive interface design and dark patterns, coercive consent mechanisms, bundled ecosystem services, addictive platform design, and opaque advertising and recommendation systems that influence consumer decision-making in ways not adequately contemplated by the current framework. Similarly, extensive data mining, behavioural profiling, targeted advertising, recommender systems, and the creation of filter bubbles and attention-capture mechanisms may significantly affect consumer autonomy, privacy, informational self-determination, mental health, and freedom of choice, yet these forms of digitally mediated consumer harm remain largely unaddressed within the statute. Failure to account for these more complex forms of digital manipulation and platform-mediated consumer harm — combined with the statute's continued focus on conventional transactional models — risks leaving consumers vulnerable to exploitation without adequate legal remedies or effective avenues for redress. More broadly, the exclusionary and technologically outdated framing of the statute may result in unequal and inconsistent treatment of consumers depending on whether transactions occur through traditional or digital channels, potentially raising concerns relating to fairness, equality, and effective protection of consumer rights within the digital economy.

RECOMMENDATIONS

Amend the definition.

Expand and modernize the definition of "anti-consumer right practice." Amend section 2(20) to include digital-specific consumer harms, such as algorithmic manipulation, deceptive pricing based on user data, and dark patterns designed to influence consumer behavior. **Certain exclusionary, exploitative, and manipulative digital practices should be expressly classified as anti-consumer right practices**, including, for instance:

(a) use of personal data, behavioural profiling, or bundled ecosystem services to facilitate discriminatory pricing, exploitative targeting, or differential treatment of consumers (*see* disclosure orders issued to eight companies for surveillance pricing, and Orbitz using steering strategies to advertise expensive hotel options to Apple users, in the United States).

(b) non-transparent or manipulative algorithmic systems, including biased search rankings, recommender systems, self-preferencing, and preferential treatment of affiliated products or services that distort consumer choice or market visibility (*see*, for instance, *Google v. Germany*, and complaint filed against Temu and decision against Amazon in the European Union; the European Commission also initiated investigation into potential breaches by Google in demoting media publishers' content in search results, while fining the company €2,950,000,000 over abusive practices in online advertising technology).

(c) excessive collection, combination, and monetization of personal and non-personal data through coercive click-through agreements, bundled consent mechanisms, or opaque data-sharing practices for advertising, profiling, pricing, or platform optimization purposes (*Meta v. Bundeskartellamt*; *Bundeskartellamt v. Facebook* in the Court of Justice in the European Union; *see*, in relation to the Cambridge Analytica scandal: (a) the settlement for US$ 100,000,000 reached by Meta with the Securities and Exchange Commission for making misleading disclosures regarding the risk of misuse of user data, and other settlement reached in October 2023 in the *Consumer Privacy User Profile Litigation*, in the United States; (b) the lawsuit initiated by the Australian Information Commissioner against Meta in Australia; and (c) the investigation into the use of data analytics in political campaigns and report on personal information and political influence by the Information Commissioner in the United Kingdom).

(a) use of dark patterns and manipulative interface design — including confusing consent flows, repeated nudging, deceptive button placement, disguised advertising, exploitative default settings, obstructive cancellation processes, and misleading subscription practices — intended to impair informed consumer choice or autonomy (*see* *Federal Trade Commission v. Amazon.com, Inc.* and the settlement agreement between the District of Columbia and Google to resolve a lawsuit involving dark pattern allegations in the United States; *see also* cases related to use of dark pattern against *Nintendo of America Inc.* for compelling users to make in-app microtransactions and *Re Epic Games, Inc.* for discouraging cancellations and refunds, the latter case settled for US$ 520,000,000).

Modernizing the statute to address digitally mediated consumer harms would help ensure that sophisticated forms of data-driven exploitation, manipulative platform conduct, and algorithmic consumer harms fall within meaningful regulatory oversight, while enabling consumers in digital markets to enjoy protections equivalent to those available in traditional commercial environments, consistent with principles of fairness, equality, transparency, and effective access to remedies. Additionally, the DNCRP should be expressly empowered to issue issue-specific rules, codes of practice, advisory guidelines, and sectoral standards relating to emerging digital consumer harms — including dark patterns, algorithmic transparency, online advertising, recommender systems, data exploitation, influencer marketing, and AI-enabled consumer manipulation — through delegated legislation and following transparent public consultation processes, thereby allowing the regulatory framework to adapt more effectively to rapidly evolving digital ecosystems without requiring frequent legislative amendment.

B. ESSENTIAL ENACTMENTS

Online Safety Act

OBJECTIVE AND RATIONALE FOR ENACTMENT

Existing legal frameworks are conceptually fragmented, technologically outdated, and institutionally ill-equipped to effectively address the scale, complexity, and transnational nature of harmful online content, platform-mediated harms, and contemporary cybercrimes. Particularly, these frameworks rely excessively on broad criminalization, vague and overbroad definitions, discretionary executive authority, and reactive takedown and platform-blocking approaches, while insufficiently addressing systemic digital risks, platform design, transparency, procedural safeguards, and institutional accountability. Current frameworks also fail to adequately distinguish between user-generated and professionally curated digital ecosystems, despite the materially different risk profiles, moderation structures, and distribution models associated with such services. Accordingly, the recommendation centers on the enactment of a unified, technologically contemporary, systems-based, and rights-respecting online safety and cybercrime framework capable of coherently regulating content-related and non-content-related digital harms within a single statutory architecture, while adopting differentiated obligations proportionate to platform type, functionality, technical architecture, and systemic risk exposure.

A comprehensive online safety statute should address the increasing challenges posed by harmful online content and platform-mediated harms (including algorithmically amplified abuse, AI-enabled manipulation, and technology-enabled exploitation), while strengthening user safety, systemic accountability, and institutional resilience within digital ecosystems. It should establish objective, proportionate, and risk-based standards and obligations applicable to users and digital platforms — including user-generated content platforms, curated streaming and subscription services, online intermediaries, app stores, messaging services, AI-enabled systems, recommender systems, hosting providers, and other digital communication channels — while carefully balancing freedom of expression, privacy, public safety, dignity, and constitutional protections against overbroad restrictions, arbitrary enforcement, and systemic censorship.

Rather than relying primarily on broad criminal prohibitions and reactive content-removal mandates, the statute should adopt a systems- and design-based regulatory approach focused on mitigating foreseeable and systemic online harms through platform risk assessments, safer product and interface design, algorithmic accountability, transparency obligations, age-appropriate design standards, user empowerment tools, friction and virality controls, trusted flagger systems, safety-by-design obligations, and proportional mitigation measures tailored to platform size, functionality, and systemic risk exposure.

Specifically, with respect to user-generated content, the statute should:

(A) clearly define the categories of digital platforms, online intermediaries, AI-enabled systems, communication services, hosting services, app stores, and recommender systems, as well as classes of regulated user-generated content and conduct covered by the framework, while differentiating obligations based on platform size, functionality, reach, and systemic risk profile;

(B) establish proportionate and risk-based duties of care requiring digital platforms to assess, mitigate, prevent, and respond to systemic online harms, including mechanisms for notice-and-action, rapid response to unlawful content, mandatory platform risk assessments, safety-by-design obligations, age-appropriate design standards, child safety protections, recommender-system accountability, virality mitigation measures, friction mechanisms, crisis response protocols, transparency obligations, and safeguards against algorithmic amplification of harmful content;

(C) establish a clear, accessible, and time-bound notice-and-action regime requiring digital platforms to expeditiously review and act upon lawful notices by government relating to unlawful content, CSAM, TFSV, technology-facilitated gender-based violence, cyberbullying, online radicalization, image-based abuse, impersonation, fraud, disinformation campaigns, and other serious harms, while incorporating procedural safeguards, counter-notice mechanisms, transparency obligations, anonymity and anti-doxxing safeguards, and protections against arbitrary or abusive takedown requests;

(D) provide accessible, user-friendly, and multilingual procedures for reporting online harms by users, obtaining remedies, contesting moderation decisions, appealing platform enforcement actions, and securing emergency assistance in serious harm cases;

(E) mandate periodic and publicly accessible transparency reporting relating to content moderation, automated enforcement systems, algorithmic recommendation systems, advertising practices, political advertising, automated decision-making, complaints received, government requests, enforcement actions, content amplification practices, and systemic platform risks;

(F) establish enhanced and differentiated protection mechanisms for vulnerable groups — including children, women, journalists, minorities, LGBTQ+ communities, persons with disabilities, and other marginalized populations — against digitally mediated harms.

Additionally, with respect to professionally curated, subscription-based, and non-user-generated content services, the statute should:

(A) establish differentiated regulatory obligations for professionally curated and editorially controlled digital services, recognizing that such platforms generally present different moderation, amplification, and systemic risk considerations than open user-generated content ecosystems;

(B) require content classification systems, recommendation practices, age-rating mechanisms, advertising disclosures, sponsored content, and parental control functionalities, and associated transparency mandates;

(C) establish age-appropriate access controls, child safety obligations, accessibility requirements, and safeguards against manipulative recommendation or autoplay systems targeting children and vulnerable users;

(D) impose obligations relating to transparency of recommender systems, algorithmic curation practices, advertising placement, and promotional prioritization where such systems materially influence user behaviour or access to information;

(E) ensure that platform obligations remain proportionate and do not undermine editorial freedom, media plurality, encryption, or legitimate artistic, journalistic, educational, cultural, or political expression.

For institutional oversight, coordination, and enforcement, the statute should:

(A) establish an independent, transparent, and technically specialized regulatory authority (or clearly delineate responsibilities among existing regulators), with powers to oversee compliance, conduct audits, require independent risk assessments, access platform data for supervisory purposes, issue guidance, impose penalties, and coordinate cross-border enforcement and regulatory cooperation;

(B) establish institutional mechanisms for coordination among regulators, LEAs, civil society organizations, academia, researchers, child protection bodies, technical experts, and digital platforms at both domestic and international levels, including trusted flagger and independent researcher access frameworks;

(C) outline lawful, proportionate, and rights-respecting procedures governing cooperation between digital platforms and LEAs in relation to investigations, evidence preservation, lawful access requests, digital evidence handling, emergency disclosure requests, and prosecution of online offenses, while safeguarding encryption, cybersecurity, and user privacy.

For cybercrime, cybersecurity, and digital infrastructure protection, the statute should, without duplicating existing offenses or compliance obligations under personal data protection, telecommunications, financial, procedural, or sector-specific legislation:

(A) criminalize unlawful access to, interference with, disruption of, or damage to digital systems, devices, communications infrastructure, cloud environments, AI systems, databases, and computer networks, including hacking, malware deployment, ransomware, botnets, denial-of-service attacks, unauthorized system intrusion, unauthorized data extraction or modification, spyware deployment, unlawful interception, cyberstalking, biometric misuse, and attacks targeting critical information infrastructure and essential digital services (such as telecommunications, energy, healthcare, finance, transportation, electoral systems, and public digital infrastructure);

(B) criminalize cyber-enabled fraud and deception offenses, including phishing, identity theft, synthetic identity fraud, online financial fraud, business email compromise, impersonation, spoofing, cryptojacking, AI-enabled fraud schemes, manipulation of digital credentials, and other technology-enabled economic offenses targeting individuals, businesses, or public institutions;

(C) establish mandatory cybersecurity risk management obligations, baseline cybersecurity standards, cybersecurity-by-design requirements, secure software development obligations, supply-chain security measures, patch management requirements, access control standards, secure default configurations, encryption protections, and resilience obligations applicable to critical infrastructure operators, cloud service providers, digital platforms, AI-enabled systems, connected devices, and other high-risk digital services;

(D) establish mandatory and time-bound cyber incident and data breach reporting obligations, coordinated vulnerability disclosure frameworks, cyber emergency response coordination systems, sector-specific resilience requirements, and legal protections for good-faith cybersecurity research, security testing, encryption use, and responsible vulnerability disclosure activities;

(E) establish lawful, proportionate, and rights-respecting procedures governing digital evidence preservation, forensic collection, admissibility of electronic evidence, emergency disclosure requests, lawful access requests, cross-border cooperation, mutual legal assistance, and cooperation with offshore digital service providers in cybercrime investigations and prosecutions, while ensuring robust safeguards relating to legality, necessity, proportionality, transparency, accountability, prior independent judicial authorization, independent oversight, due process, encryption protection, cybersecurity integrity, and protection of fundamental rights;

(F) establish coordinated public-private cyber defense, preparedness, and resilience mechanisms involving regulators, cybersecurity agencies, law enforcement authorities, critical infrastructure operators, private sector entities, academia, civil society, and technical experts, including information-sharing frameworks, coordinated threat intelligence systems, incident response and recovery frameworks, sectoral cyber resilience programs, and specialized cybercrime investigation, prosecution, judicial, and digital forensic capacity-building mechanisms.

A unified and coherent framework combining preventive, systems-based, regulatory, remedial, and criminal enforcement mechanisms would better enable Bangladesh to address evolving online harms and cyber threats while preserving an open, secure,

rights-respecting, interoperable, and innovation-friendly digital ecosystem aligned with emerging comparative international approaches to online safety and cybersecurity governance.

COMPARABLE LAWS

Australia

1) *Online Safety Act 2021*
2) *Online Safety (Basic Online Safety Expectations) Determination 2022*
3) Basic Online Safety Expectations
4) Adult Cyber Abuse Scheme
5) Abhorrent Violent Conduct Powers Regulatory Guidance
6) Online Content Scheme
7) Image-Based Abuse Scheme
8) Cyberbullying Scheme

European Union

9) *Digital Services Act*
10) *Artificial Intelligence Act*
11) *Directive on Combating Violence Against Women and Domestic Violence*
12) *Audiovisual Media Services Directive*
13) *Regulation on Dissemination of Terrorist Content Online*
14) *Regulation on Political Advertising Transparency and Targeting*
15) Code of Conduct on Disinformation

Singapore

16) *Broadcasting Act 1994*
17) *Online Criminal Harms Act 2023*
18) *Protection from Online Falsehoods and Manipulation Act 2019*
19) *Foreign Interference (Countermeasures) Act 2021*
20) Code of Practice for Online Safety
21) Guidelines on Categories of Harmful Content

United Kingdom

22) *Online Safety Act 2023*
23) *Media Act 2024*
24) *Age-Appropriate Design Code of Practice for Online Services*

United States

25) *American Innovation and Choice Online Bill*
26) *Kids Online Safety Bill*

Regulation of Investigatory Powers Act

OBJECTIVE AND RATIONALE FOR ENACTMENT

Bangladesh's existing framework on investigatory powers, surveillance, interception, communications monitoring, and intelligence gathering remains fragmented across multiple statutes, licences, executive instruments, and non-public agency mandates, collectively conferring wide discretionary powers without sufficiently clear legal thresholds, independent authorization, oversight, transparency, or redress mechanisms.

Currently, the Intelligence Agencies and other LEAs in Bangladesh are actively involved in surveillance, interception, and intelligence gathering activities — and this includes NSI, NTMC, BTRC, BFIU, and DGFI, as well as specialized units within the Bangladesh Police like the Special Branch, Detective Branch, Criminal Investigation Department, and Counter Terrorism and Transnational Crime unit. The authority to undertake these activities stems from three broad sources.

First, LEAs derive extensive investigative powers from colonial- and post-independence-era statutes, particularly the *Code of Criminal Procedure, 1898* and the *Special Powers Act, 1974*, which are frequently incorporated or reinforced through later sector-specific statutes.

Secondly, special laws — including the *Bangladesh Telecommunication Act, 2001*, the *Anti-Terrorism Act, 2009*, the *Money Laundering Prevention Act, 2012*, and related sectoral frameworks — authorize or facilitate access to communications data, subscriber information, financial intelligence, interception capability, and service-provider cooperation. Together with telecommunications licences and regulatory directives, these instruments create a compliance architecture through which private actors may be required to assist state surveillance, interception, and disclosure activities.

Thirdly, certain Intelligence Agencies, including DGFI, NSI and NTMC, appear to operate through mandates, executive arrangements, inter-ministerial instruments, or internal rules that are not fully public, accessible, or subject to ordinary legislative scrutiny, creating significant concerns regarding legality, foreseeability, institutional accountability, and democratic oversight.

While the Constitution permits reasonable restrictions on certain rights on grounds such as national security, public order, and related public interests, surveillance, interception, and investigatory powers must still satisfy core rule-of-law requirements of legality, necessity, proportionality, legitimate aim, independent authorization, and effective oversight. Because the existing framework does not adequately embed these requirements, or other procedural safeguards like data minimization, retention limits, auditability, or accountability, it risks enabling arbitrary or disproportionate interference with privacy, freedom of expression, freedom of association, journalistic confidentiality, lawyer-client privilege, due process, and fair trial rights. This highlights the urgent need for legislative reform to establish a more balanced, future-proof, and rights-respecting approach to surveillance, interception, and intelligence gathering in Bangladesh.

Given the expansion of surveillance, interception, metadata access, device monitoring, financial intelligence, and digital investigation capabilities over the past two decades, Bangladesh should conduct an independent national review and public consultation on all legal, regulatory, licensing, procurement, and executive instruments enabling these activities. Specifically, the review and consultation should consider:

(A) establishment of a robust personal data protection legislation, consistent with international best practices and conventions, tailored to meet relevant policy considerations and constitutional requirements, aimed at mitigating the risks of abusive surveillance, interception, and intelligence gathering practices; and this includes its meaningful implementation to public-sector

processing, especially to the LEAs and the Intelligence Agencies, subject only to narrowly tailored exemptions grounded in legality, necessity, proportionality, independent oversight, and effective remedies; and

(B) the repeal, amendment, or consolidation of fragmented surveillance, interception, disclosure, lawful access, intelligence-gathering, and investigative powers into a single statute that harmonizes state security with fundamental rights, international human rights standards, and democratic accountability.

A consolidated investigatory, surveillance, interception, and intelligence-gathering statute should, at minimum:

(A) clearly define the specific circumstances in which state agencies may conduct communications interception, metadata access, device search, geolocation tracking, financial intelligence access, remote access, or other forms of surveillance and interception, and limit such powers to serious offences, genuine national security threats, or clearly defined emergency situations, with prior authorization by an independent court or judicial authority, subject only to narrowly defined emergency exceptions requiring prompt post-facto judicial approval;

(B) require every authorization request to specify the legal basis, legitimate aim, target identity or identifier, necessity, proportionality, scope, duration, type of data sought, technical method, service provider obligations, minimization measures, safeguards for privileged or sensitive communications, and an express constitutional and human rights compliance certification demonstrating that the requested measure is consistent with applicable constitutional guarantees, statutory safeguards, and Bangladesh's international human rights obligations;

(C) prohibit bulk, indiscriminate, or untargeted surveillance except under an exceptional statutory framework with heightened necessity and proportionality requirements, prior independent authorization, parliamentary oversight, technical safeguards, periodic review, and strict limits on search, retention, and dissemination;

(D) establish strict duration limits, renewal standards, data minimization requirements, retention and deletion rules, access logs, audit trails, and purpose limitation obligations for all intercepted or acquired information;

(E) protect legally privileged, journalistic, parliamentary, medical, human rights, and other sensitive communications through heightened authorization standards and special handling safeguards;

(F) create layered oversight mechanisms, including prior judicial authorization, an independent surveillance commissioner or inspector-general, parliamentary committee oversight, periodic independent audits, annual public transparency reporting, classified reporting to parliament, and enforceable internal compliance systems;

(G) require telecommunications operators, digital platforms, financial institutions, and other service providers to cooperate only pursuant to lawful, written, reviewable, and narrowly tailored orders, while prohibiting informal, oral, extra-legal, or politically directed requests for user data or interception assistance;

(H) establish clear rules for cross-border data requests, intelligence sharing, mutual legal assistance, emergency disclosure, and cooperation with foreign governments, ensuring legality, reciprocity, human rights safeguards, data protection, onward-transfer restrictions, and independent review;

(I) provide effective remedies for unlawful surveillance, including notification to affected persons where doing so no longer prejudices an investigation, access to an independent complaints body, judicial review, exclusion of unlawfully obtained evidence, compensation, disciplinary sanctions, and criminal penalties for intentional or reckless misuse of surveillance powers;

(J) mandate publication of aggregate transparency statistics on surveillance orders, interception requests, metadata access, emergency requests, foreign cooperation requests, approvals, refusals, renewals, and compliance actions, subject only to narrowly tailored redactions necessary to protect ongoing investigations or legitimate national security interests;

Regulation of Investigatory Powers Act

(K) require procurement, deployment, and use of surveillance technologies — including spyware, IMSI catchers, facial recognition, biometric systems, social media monitoring tools, AI-enabled analytics, and data-fusion platforms — to be expressly authorized by law, subject to human rights impact assessments, procurement transparency, independent technical audits, and restrictions on use against journalists, political opponents, activists, lawyers, and marginalized communities;

(L) clearly allocate institutional responsibilities among LEAs, Intelligence Agencies, regulators, prosecutors, courts, and oversight bodies to avoid overlapping mandates, informal surveillance channels, and accountability gaps.

COMPARABLE LAWS

Australia

1) *Telecommunications (Interception and Access) Act 1979*
2) *Surveillance Devices Act 2004*
3) *Australian Security Intelligence Organisation Act 1979*
4) *Telecommunications Act 1997*
5) *Crimes Act 1914*

European Union

6) *Law Enforcement Directive*
7) *Directive on Privacy and Electronic Communications*
8) *NIS 2 Directive*

Germany

9) *Act Restricting the Privacy of Correspondence, Posts and Telecommunications 2001*

Japan

10) *Act on Communications Interception for Criminal Investigation*

New Zealand

11) *Intelligence and Security Act 2017*
12) *Search and Surveillance Act 2012*
13) *Telecommunications (Interception Capability and Security) Act 2013*

United Kingdom

14) *Investigatory Powers Act 2016*
15) *Regulation of Investigatory Powers Act 2000*
16) *Data Retention and Investigatory Powers Act 2014*
17) *Protection of Freedoms Act 2012*
18) *Telecommunications Act 1984*
19) *Code of Practice on Covert Surveillance and Property Interference*

Digital Commerce Act

OBJECTIVE AND RATIONALE FOR ENACTMENT

Currently, regulation of digital commerce remains fragmented and overly reliant on soft-law instruments such as policies, guidelines, and voluntary codes of conduct, which, despite offering flexibility, lack binding force, institutional accountability, enforcement consistency, and legal certainty. Although certain existing statutes — such as the *Competition Act, 2012* and the *Consumers' Right Protection Act, 2009*, addressed above — indirectly regulate aspects of competition, consumer protection, unfair trade practices, and commercial conduct within digital markets, these frameworks remain largely rooted in traditional conceptions of commerce and consumer relationships and are therefore insufficiently equipped to address the realities of contemporary digital commerce ecosystems. As such, Bangladesh still lacks a comprehensive, technologically contemporary legal framework specifically governing digital commerce. This regulatory gap enables platforms and businesses to exploit ambiguities, while leaving consumers vulnerable to fraud, misleading advertising, unsafe products, opaque pricing, unfair contractual terms, manipulative interface design, poor-quality services, and inadequate dispute-resolution mechanisms.

A central weakness of the existing framework is the absence of clear, technologically neutral, and function-based definitions capable of capturing the wide range of digital commerce services, intermediaries, and platform ecosystems operating in Bangladesh. As currently framed, it remains unclear, for instance, whether platforms such as Facebook, Instagram, WhatsApp, TikTok, or Telegram — which facilitate commercial activity, advertising, livestream sales, influencer-driven commerce, or marketplace interactions without necessarily processing transactions directly — fall within the scope of existing e-commerce regulation. These gray zones undermine legal certainty, market fairness, taxation, consumer protection, and enforceability, while also complicating cross-border digital trade in conjunction with restrictive customs, payment, and foreign exchange regimes.

Digital commerce services operate through diverse techno-commercial models with significantly different technical architectures, operational structures, risk profiles, payment systems, logistics arrangements, intermediary functions, and target market, necessitating differentiated and platform-sensitive governance rather than a one-size-fits-all regulatory approach. These include, for instance:

(A) business-to-consumer (B2C) models such as Amazon or Daraz, involving integrated marketplaces, escrow services and payment gateways, logistics, recommendation systems, and direct consumer sales;

(B) business-to-business (B2B) models such as Alibaba, facilitating enterprise procurement, wholesale transactions, customized pricing, escrow services and payment gateways, and supply-chain integration;

(C) consumer-to-consumer (C2C) and social commerce models such as Facebook Marketplace, TikTok Shop, eBay, or Craigslist, relying on peer-to-peer interactions, targeted advertising, influencer marketing, livestreaming, and platform recommendation systems, sometimes with escrow services and payment gateways;

(D) consumer-to-business (C2B) models such as Upwork or Shutterstock, enabling platform-mediated provision of services, labor, or digital content by individuals to businesses, often with escrow services and payment gateways;

(E) business-to-business-to-consumer (B2B2C) ecosystems such as Shopify-enabled marketplaces or third-party seller ecosystems operating through Amazon;

(F) mobile commerce and super-app ecosystems such as bKash, Uber, Pathao, or app-based delivery platforms, which rely on integrated payments, geolocation systems, app-based contracting, and multi-service integration.

Additional models — including business-to-government (B2G) and government-to-consumer (G2C) services, subscription commerce, gig economy platforms, digital content marketplaces, creator economies, and cross-border digital marketplaces — similarly require differentiated regulatory treatment depending on their functionality, operational control, payment structure, and systemic role.

Significant differences also exist within the same category of services. For instance, while both Facebook Marketplace and TikTok Shop operate as C2C model, the former primarily facilitates advertising and offline peer-to-peer transactions, whereas TikTok Shop integrates on-platform payments, recommendation systems, logistics, and fulfillment services. Such differences necessitate carefully calibrated obligations tailored to the functionality, level of control, and systemic role of different platforms and intermediaries.

A comprehensive digital commerce framework would enhance legal certainty, consumer trust, market fairness, cross-border interoperability, and investment predictability, while protecting constitutional guarantees relating to property, privacy, access to justice, freedom of contract, and the right to engage in lawful trade and business without unreasonable restrictions.

Accordingly, there is a need to:

(A) enact a comprehensive, technologically neutral, and platform-aware digital commerce statute capable of accommodating diverse techno-commercial models, digital intermediaries, online marketplaces, social commerce platforms, livestream commerce, app-based services, AI-enabled commercial systems, and cross-border digital trade ecosystems;

(B) establish clear and narrowly tailored extraterritorial provisions applicable to offshore digital commerce platforms and intermediaries providing services to users within Bangladesh, while minimizing jurisdictional overreach and conflicting compliance obligations;

(C) harmonize related frameworks governing customs, taxation, foreign exchange, digital payments, consumer protection, contracts, competition, cybersecurity, data protection, intermediary liability, logistics, and intellectual property to ensure coherent enforcement and facilitate domestic and cross-border digital trade;

(D) establish clear rules governing electronic contracts, digital signatures, automated transactions, platform terms of service, click-wrap agreements, return and refund obligations, statutory guarantees, intermediary liability protections, and online dispute-resolution mechanisms;

(E) modernize customs, taxation, and cross-border trade procedures through digitized customs systems, simplified low-value shipment procedures, interoperable payment and logistics infrastructure, transparent tariff structures, and anti-corruption safeguards;

(F) incorporate safeguards against fraud, counterfeit products, unsafe goods, deceptive pricing, dark patterns, fake reviews, influencer marketing abuses, manipulative recommendation systems, discriminatory pricing, algorithmic manipulation, AI-generated scams, and other emerging forms of digital consumer harm;

(G) introduce platform transparency and accountability obligations relating to seller verification, traceability of commercial actors, sponsored advertising disclosures, recommender systems, ranking criteria, automated decision-making, and targeted advertising practices;

(H) establish minimum cybersecurity, payment security, consumer data protection, and fraud-prevention standards for digital commerce platforms, payment gateways, logistics providers, and digital intermediaries;

(I) require interoperable and accessible online

dispute-resolution and consumer complaint mechanisms, including mandatory response timelines, transparent refund procedures, and low-cost redress systems for consumers and small businesses;

(J) introduce due diligence and notice-and-action obligations for marketplaces and intermediaries in relation to counterfeit products, unlawful goods, fraudulent sellers, intellectual property violations, and unsafe products, while preserving proportionate intermediary liability protections;

(K) establish proportionate civil, administrative, and criminal liability mechanisms calibrated to the severity and systemic impact of the harm involved, alongside effective regulatory enforcement powers and accessible consumer redress systems.

COMPARABLE LAWS

European Union

1) *Digital Markets Act*
2) *Digital Services Act*
3) *Consumer Rights Directive*
4) *Platform-to-Business (P2B) Regulation*
5) *General Product Safety Regulation*
6) *Consumer Credit Directive and Digital Content & Digital Services Directive*
7) *Omnibus Directive*

Organisation for Economic Co-operation and Development

8) Recommendation of the Council on Consumer Protection in E-commerce

United Nations

9) *United Nations Convention on the Use of Electronic Communications in International Contracts*
10) UNCITRAL Model Law on Electronic Commerce

United Kingdom

11) *Digital Markets, Competition and Consumers Act 2024*
12) *Electronic Commerce (EC Directive) Regulations 2002*
13) *Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013*
14) *Consumer Protection from Unfair Trading Regulations 2008*

United States

15) *Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Act*
16) Guides Concerning the Use of Endorsements and Testimonials in Advertising
17) *The Electronic Signatures in Global and National Commerce Act*
18) Strategic Plan 2022 - 2026 on Innovation, Equity, and Resilience: Strengthening American Competitiveness in the 21st Century

Artificial Intelligence Strategy

OBJECTIVE AND RATIONALE FOR ENACTMENT

The rapid design, deployment, integration, and commercialization of AI systems across public and private sectors require the development of a comprehensive national governance framework capable of addressing the legal, constitutional, social, economic, institutional, security, and business implications arising from increasingly pervasive AI-enabled systems. Increasingly, these systems are now being integrated into judicial administration, policing, healthcare, education, financial services, labor and recruitment, public administration, border control, social protection, critical infrastructure, defense, media, and digital platform ecosystems, creating significant opportunities alongside substantial risks to fundamental rights, democratic governance, economic fairness, and public trust.

For example, AI-assisted judicial or administrative decision-making requires heightened safeguards relating to due process, explainability, contestability, transparency, and judicial independence. Similarly, healthcare applications raise issues of privacy, informed consent, reliability, medical accountability, and algorithmic safety, while educational systems implicate equality, accessibility, and non-discrimination concerns. Moreover, generative AI systems, recommender systems, synthetic media, deepfakes, and predictive surveillance technologies increasingly intersect with information integrity, electoral processes, freedom of expression, cybersecurity, labor displacement, and constitutional protections against arbitrary or disproportionate intrusion into individual autonomy and privacy.

At this stage of technological and regulatory evolution, Bangladesh should avoid prematurely adopting rigid technology-specific legislation and instead prioritize a flexible, adaptive, and principles-based soft-law governance framework capable of evolving alongside technological developments and international standards. Initially, this should take the form of national AI strategies, ethical guidelines, technical standards, regulatory sandboxes, sectoral codes of conduct, certification schemes, procurement standards, impact assessment frameworks, and coordinated sector-specific guidance before considering comprehensive statutory regulation. Such an approach would allow regulators, industry, academia, civil society, and technical experts to develop institutional expertise, iteratively test governance approaches, and respond dynamically to technological developments without creating obsolete or innovation-stifling legal frameworks.

Moreover, the governance framework should remain context-specific and risk-sensitive rather than treating AI as a monolithic technology category. Accordingly, both national and sectoral frameworks should balance innovation, investment, and competitiveness with accountability, transparency, consumer protection, privacy, labor protections, cybersecurity, non-discrimination, democratic integrity, and protection against harmful or irresponsible deployment of such systems. Regulatory approaches should therefore be tailored to the context, capability, deployment environment, degree of autonomy, scale of impact, and foreseeable risks associated with particular AI systems and use-cases

Accordingly, a national AI governance framework should establish foundational principles and minimum governance standards requiring AI systems and services to:

(A) be grounded in rights-respecting principles, including legality, accountability, transparency, explainability, contestability, fairness, inclusivity, reliability, robustness, safety, security, human oversight, and conformity with constitutional guarantees and international human rights standards;

(B) adopt a human-centered governance approach that preserves human dignity, autonomy, democratic

participation, societal welfare, and environmental sustainability rather than purely commercial or authoritarian objectives;

(C) balance innovation, investment, research, and economic competitiveness with consumer protection, labor protections, privacy, cybersecurity, equality, non-discrimination, and other fundamental rights through multi-stakeholder governance involving regulators, lawmakers, technical experts, academia, industry, civil society, marginalized communities, labor representatives, journalists, and independent researchers;

(D) remain interoperable and aligned with emerging international standards and governance best practices to facilitate cross-border cooperation, responsible innovation, and participation in evolving global AI governance processes.

Particularly, the framework should additionally:

(E) adopt a risk-based and context-sensitive regulatory approach distinguishing between prohibited, high-risk, limited-risk, and minimal-risk AI systems;

(F) prohibit or strictly limit particularly harmful AI practices, including unlawful biometric mass surveillance, social scoring, discriminatory profiling, exploitative systems targeting vulnerable populations, unlawful predictive policing, and AI systems that materially undermine democratic participation or constitutional rights;

(G) require algorithmic, human rights, privacy, and safety impact assessments for high-risk AI systems prior to deployment within sensitive sectors;

(H) require meaningful human oversight, explainability, contestability, and accessible remedies for AI-assisted decisions materially affecting rights, liberty, employment, healthcare, education, credit, housing, or democratic participation;

(I) establish transparency obligations requiring disclosure where individuals interact with AI systems or AI-generated content, including appropriate labeling obligations for deepfakes and synthetic media;

(J) promote responsible public-sector AI procurement and deployment standards, including fairness testing, security auditing, documentation obligations, and independent review mechanisms for high-risk government AI systems;

(K) encourage regulatory sandboxes, certification mechanisms, independent testing environments, and sector-specific technical guidance to support innovation while maintaining accountability and public trust;

(L) require robust cybersecurity, adversarial testing, incident reporting, and safeguards against model misuse, manipulation, and unauthorized access;

(M) support open research, public-interest innovation, local language AI development, accessibility technologies, digital inclusion, and capacity-building initiatives;

(N) establish institutional coordination mechanisms to periodically update governance approaches and ensure ongoing constitutional, ethical, and societal oversight of AI systems.

COMPARABLE LAWS

Australia

1) National Framework for the Assurance of Artificial Intelligence in Government
2) Voluntary AI Safety Standard
3) Proposed Paper on Safe and responsible AI in Australia

Canada

4) *Artificial Intelligence and Data Bill*
5) *Companion document on Artificial Intelligence and Data Act*
6) *Directive on Automated Decision-Making 2019*

Council of Europe

7) The Framework Convention on Artificial Intelligence

European Union

8) Artificial Intelligence Act

9) Guidelines on the Scope of the Obligations for General-Purpose AI models

10) General-Purpose AI Code of Practice 2025

Global Partnership on Artificial Intelligence

11) 2024 GPAI New Delhi Declaration

Indonesia

12) 2020–2045 Artificial Intelligence National Strategy

Japan

13) AI Strategy 2022

14) Report from the Expert Group on How A Principles Should be Implemented

New Zealand

15) Algorithm Charter for Aotearoa New Zealand

Organisation for Economic Co-operation and Development

16) Recommendation of the Council on Artificial Intelligence

17) G7 Hiroshima Process on Generative Artificial Intelligence

Singapore

18) National Strategy on AI for the Public Good For Singapore and the World

19) Model AI Governance Framework for Generative AI

United Kingdom

20) National AI Strategy

21) A Pro-Innovation Approach to AI Regulation

United Nations

22) Interim Report on Governing AI for Humanity

23) United Nations System White Paper on AI Governance

United Nations Educational, Scientific and Cultural Organization

24) Recommendation on the Ethics of Artificial Intelligence

United States

25) National Artificial Intelligence Initiative Act of 2020

26) Algorithmic Accountability Bill

27) Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile

28) Blueprint for an AI Bill of Rights Making Automated Systems Work for the American People

29) Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government

30) Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

31) Executive Order on Maintaining American Leadership in Artificial Intelligence

TECHGLOBAL INSTITUTE

techglobalinstitute.com