A NEW DIGITAL FRONTIER

A Blueprint for Reforms towards Rights-Respecting Information and Technology Laws in Bangladesh

Shahzeb Mahmood & **Sabhanaz Rashid Diya**

WHITE PAPER

A New Digital Frontier: A Blueprint for Reforms towards Rights-Respecting Information and Technology Laws in Bangladesh

Shahzeb Mahmood & Sabhanaz Rashid Diya

Copyediting by Afia Jahin
Publication design by Subinoy Mustofi
Cover artwork by DELL-E

TECHGLOBAL INSTITUTE

techglobalinstitute.com

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 Regulation 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 content, including still images, videos, audio recordings, and digital media, that visually or audibly minors engaged in sexual activity, or otherwise represents minor in a sexually explicit manner.
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.
GAFAM	is the acronym for five major technology companies, namely, Google (Alphabet), Apple, Facebook (Meta), Amazon, and Microsoft.
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.

ABBREVIATIONS

Intelligence Agencies	means government organizations tasked with gathering, analyzing, and managing information related to national security, foreign affairs, and internal threats, and engaging in surveillance, espionage, and counterintelligence, including, without limitation, BFIU, BTRC, DGFI, NCSA, 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.
LEA	means law enforcement agencies, including Bangladesh Police, as well as the Intelligence Agencies.
NSI	means the National Security Intelligence, the civilian intelligence agency of Bangladesh, operating under the Prime Minister's Office.
NCSC	means National Cyber Security Council established under the Cyber Security Act, 2023 (Act No. XXXIX of 2023).
NCSA	means National Cyber Security Agency established under the Cyber Security Act, 2023 (Act No. XXXIX of 2023), and, accordingly, DG-NCSA should be construed as Director General of the National Cyber Security Agency.
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, investigatory authority, 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 three 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 five key legislations that underpin the existing regulatory environment: the *Penal Code, 1860*, the *Pornography Control Act, 2012*, the *Competition Act, 2012*, the *Consumer Rights Protection Act, 2009*, and the *Bangladesh Telecommunication Regulation Act, 2001*. These revisions aim to modernize outdated provisions, address definitional ambiguities, and enhance their effectiveness in the digital age.

Part B examines the urgent need for the repeal of the *Cyber Security Act, 2023*, highlighting its deficiencies and recommending its replacement with a more balanced and rights-respecting framework.

Part C outlines essential enactments required to address gaps in the legal landscape, proposing four new legislations: the *Online Safety Act*, the *Regulation of Investigatory Powers Act*, the *Personal Data Protection Act*, the *Digital Commerce Act*, and a forward-looking Artificial Intelligence Strategy. Collectively, these provide a comprehensive roadmap for reform, ensuring a robust, equitable, and digital-first legal system.

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 determined and utilized Bangladesh's Constitution and international frameworks like the *Universal Declaration for Human Rights* (UDHR), the *International Covenant on Civil and Political Rights* (ICCPR) and the *UN Guiding Principles for Business and Human Rights* (UNGPs) as key benchmarks. Although international human rights law and rule-based international order are not without criticism—often debated as "Eurocentric" through its politicized deployment by Western states and inconsistent implementation, they provide a universal foundation. International human rights law enjoys broad support from governments, civil society and technical communities, and has served as a widely recognized framework for governance norms for over 70 years.

We argue 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 a framework to mitigate specific types of harms, they are not a universal solution for addressing the complexities of diverse human conditions, ethical dilemmas, and political realities. Human discretion and contextualization are essential to ensure digital technologies serve public interest and safeguard fundamental rights.

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

The legal frameworks analyzed in this paper primarily focus on Bangladesh. However, similar patterns of colonial-era statutes, protectionism, 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 be particularly relevant and actionable in resource-constraint political environments within Global South countries.

EXECUTIVE SUMMARY

The rapid digitization in Bangladesh has not only accelerated economic growth and expanded connectivity but has also profoundly transformed social dynamics. However, these developments come with complex regulatory challenges, as the state has sought to govern this digital expansion within a legal framework that, despite reform attempts, has not fully adapted to a digital-first reality. The primary legislative instruments governing digital activities—the *Bangladesh Telecommunication Regulation Act, 2001*, the *Cyber Security Act, 2023*, the *Information and Communication Technology Act, 2006*, and other laws—present a paradox. While these laws purport to secure cyberspace and safeguard public interests, they often fall short of meeting constitutional requirements and international human rights standards, creating an environment where digital rights, innovation, and national security are simultaneously at risk. Additionally, despite their promise, laws like the *Children Act, 2013*, the *Prevention of Women and Children Repression Act, 2000*, and the *Pornography Control Act, 2012* fail to provide robust protections against pressing online abuses such as child sexual abuse materials (CSAM) and technology-facilitated sexual violence (TFSV), leaving significant gaps in addressing the unique vulnerabilities of the digital ecosystem and undermining efforts to create a safe and equitable online environment. Other legislative instruments, such as the *Competition Act, 2012* and the *Consumers' Right Protection Act, 2009*, were crafted with traditional markets in mind and fail to adequately address the complexities of the digital economy or provide sufficient protection for competitors and consumers in the digital domain.

These legislative instruments are set against the backdrop of Bangladesh's complex socioeconomic and political realities. A significant number of these laws were enacted or amended during the 16-year rule under former Prime Minister Sheikh Hasina that prioritized consolidation of the state through prioritizing political control over key institutions, including the security sector, media, and the judiciary. As a result, they failed to address structural disenfranchisement of vulnerable communities, such as women, children and minority communities that extend to online spaces and has led to multiple bouts of fatal riots, communal violence, and targeted attacks.

Of particular concern is Bangladesh's Constitution, which—despite its progressive framework inspired by globally recognized instruments such as the *International Covenant for Civil and Political Rights* (ICCPR) and the *Universal Declaration of Human Rights*, along with principles from established constitutional democracies—has been systematically exploited by successive administrations to centralize executive power while curtailing parliamentary autonomy and judicial independence. In particular, the Westminster-style parliamentary system, intended to ensure accountability through a prime minister-led cabinet answerable to parliament, has instead devolved into an apparatus dominated by the ruling party, sidelining opposition voices and consolidating decision-making authority within the executive branch. Such a systemic imbalance has facilitated unchecked executive overreach and paved the way for the enactment

of repressive laws. 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 interpretations have frequently adopted overly broad and restrictive views, particularly in defining what constitutes "reasonable" restrictions on fundamental freedoms such as speech and privacy. These interpretations often lack proportionality and fail to establish clear boundaries, undermining the protection of individual rights. Moreover, the absence of adequately reasoned judicial decisions has exacerbated ambiguity, leaving the scope and legitimacy of such restrictions open to manipulation. Collectively, these systemic failures have undermined the Constitution's role as a safeguard for democratic governance and fundamental rights.

One of the core issues in the current information and technology legislations in Bangladesh is the overbroad and ambiguous nature of its regulatory provisions, including poorly structured definitions, granting significant discretionary powers to policymakers, regulators, and law enforcement agencies (LEAs). For instance, the *Bangladesh Telecommunication Regulation Act, 2001* allows for extensive surveillance, data interception, and information control. While justified on national security or public order grounds, they are often deployed without adequate oversight mechanisms or procedural safeguards, infringing on privacy and freedom of expression. With the absence of transparency and accountability mechanisms, or robust data protection legislation, a culture of impunity has evolved with the resulting environment not only restricting fundamental freedoms but also deterring foreign investment. Moreover, crucial terms such as "propaganda," "disrepute to the state," and "hurting religious sentiments" under the *Cyber Security Act, 2023*, or "pornography" under the *Pornography Control Act, 2012*, lack clear and objective definitions, enabling subjective interpretation and selective enforcement. Consequently, these legislations have led to the criminalization of online dissent, self-censorship, suppression of opposition voices, and erosion of trust in state institutions, underscoring the urgent need for reform to better align national security priorities with citizens' fundamental rights.

The regulatory approach to digital governance in Bangladesh also reflects an overarching reliance on security-first frameworks. Key institutions, such as the National Cyber Security Agency (NCSA), operate under close ministerial supervision, with leadership from state agencies and limited representation from independent experts or civil society. Similarly, Bangladesh Telecommunication Regulatory Commission (BTRC) operates without meaningful political or structural independence, often prioritizing state control over safeguarding individual rights, compromising the agency's ability to serve as an impartial regulator. Moreover, intelligence agencies such as Directorate General of Forces Intelligence (DGFI), National Security Intelligence (NSI), and National Telecommunication Monitoring Centre (NTMC) operate without publicly accessible mandates, transparent oversight mechanisms, or clear procedural guardrails, fostering an environment of fear and self-censorship that undermines democratic governance and the protection of human rights. This security-focused framework has resulted in an imbalance, where policies aimed at securing cyberspace have not been coupled with robust protection for individual freedoms or innovation. Such an approach, in its current

form, is both misaligned with domestic constitutional obligations and inconsistent with Bangladesh's commitments under the ICCPR.

The colonial underpinning of digital governance exacerbated both enforcement and ethical challenges. For instance, the *Cyber Security Act, 2023* consolidates governmental authority over online expression, cybersecurity, and data-related offenses but does so in ways that do not adequately delineate between these offenses, and risk stifling innovation and economic growth in the digital sector. Likewise, the *Bangladesh Telecommunication Regulation Act, 2001*, originally intended to establish a regulatory framework for the telecommunications sector, has frequently been repurposed to justify surveillance and restrict digital content, often without clear statutory mandates or procedural safeguards.

Some of these laws borrow language directly from colonial-era statutes, such as the *Penal Code, 1860*, and are structurally modeled on archaic legislative paradigms like the *Code of Criminal Procedure, 1898*. For example, treating speech-related offenses as criminal offenses have fostered an environment of self-censorship, particularly among journalists, activists, and opposition voices, thereby limiting the scope of public debate and eroding democratic norms. Notably, criminal libel has been systemically used to erode the fundamental rights of citizens, serving as a weapon for political warfare both offline and online. Overbroad penal provisions, coupled with non-bailable clauses and cognizable offenses, enable LEAs to arrest individuals without warrants, often on subjective grounds and without following due process. These reflect colonial extractive values being imposed on modern rulemaking, rendering them unfit to tackle the myriad of challenges in the digital space. This creates an environment where the very foundations of governance come at the expense of protecting individual rights and advancing an innovation-friendly and inclusive digital ecosystem. This combination of inadequate safeguards and excessive penalties underscores the need for legal reforms that emphasize proportionality, judicial oversight, and procedural safeguards.

The inadequacy of laws to regulate the digital ecosystem in Bangladesh goes beyond online expression, safety and privacy, to areas like competition that are foundational in shaping the market. While countries in South and Southeast Asia, Europe, and the United States have utilized competition laws to hold technology companies accountable (to various degrees of success) by deterring the abuse of dominant positions and enhancing an environment where smaller businesses can thrive, Bangladesh's *Competition Act, 2012* remains underutilized and inadequate for addressing the challenges of the digital economy. One notable case involved an online-based food delivery service that was fined BDT 1 million (approximately USD 8,500), an amount far from sufficient to serve as a meaningful deterrent. Similarly, the *Consumer Rights Protection Act, 2009* is ill-equipped to address issues in the digital domain, as crucial definitions exclude significant portions of the digital economy, such as zero-cost digital platforms, and fails to address modern anti-consumer practices like algorithm manipulation, dark patterns, or privacy exploitation.

Bangladesh stands at a pivotal moment in shaping a digital ecosystem that aligns with global standards for human rights and accountability, while simultaneously undergoing

a decolonization exercise. The need for a comprehensive and rights-respecting approach to digital regulation is clear, as current policies often prioritize security at the expense of individual freedoms, innovation and democratic principles. By pursuing the recommended reforms, Bangladesh can develop a digital governance model that promotes security, fosters innovation, and respects the rights of its citizens.

However, legal reforms alone are insufficient to propel Bangladesh toward an inclusive, rights-respecting digital economy. Structured interventions are equally critical to address the country's deep-rooted societal challenges related to religion, ethnicity, gender, education, and income inequality. Moreover, investing in healthy and competitive media and information environments is equally important in ensuring citizens can exercise their rights. 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 regulation needs to be adaptive and context-sensitive, integrating legal, technical, and societal dimensions, while being sufficiently future-proof and technology-neutral to address new and emerging technological developments. For Bangladesh, this means not only reforming outdated and repressive laws, but also creating an enabling 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.

KEY RECOMMENDATIONS

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 the 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.

2. ***Introduce new online safety standards and procedures for content regulation.*** Existing and proposed regulations 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 for cases involving minor offenses. Harmful content, such as CSAM and TFSV, should be subject to stricter sanctions. Additionally, the *Bangladesh Telecommunication Regulation Act, 2001* should be amended to enhance the independence of BTRC, 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 repealed. Within the framework of the online safety statute, legal mechanisms to counter cybersecurity crimes—like hacking, identity theft, financial fraud, ransomwares, unauthorized data modification and access, and other offenses related to digital infrastructures and other information communications technologies—should be strengthened. Furthermore, the governance structure of cybersecurity institutions, particularly the NCSA, 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 law. Such reforms would also promote confidence in Bangladesh's digital economy, protecting both consumers and responsible businesses, while encouraging foreign investment.

5. ***Introduce a personal data protection statute.*** Currently, there is no comprehensive, cross-sectoral personal data protection statute in Bangladesh to safeguard citizens' privacy rights and establish standards for data security. A new data protection law should be enacted, outlining data processing limits, storage standards, and consent requirements, ensuring data is collected and processed responsibly by both public and private entities. Robust data protection would also enhance trust in digital services and enable Bangladesh to comply with international data protection frameworks.

6. ***Introduce sentencing guidelines, a recommendation system, and centralized case tracking system.*** Currently, there are no structures or systems to ensure balanced and consistent sentencing in criminal cases. Without sentencing guidelines or recommendation system, or 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 ensure uniformity and proportionality in the application of penalties, limit judicial discretion, and avoid arbitrary sentencing.

A PATCHWORK OF LEGISLATIONS AND SOFT LAWS

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

Censorship, and Information and Media Control

1. Part III, Constitution
2. Cyber Security Act, 2023
3. Penal Code, 1860
4. Anti-Terrorism Act, 2009
5. Pornography Control Act, 2012
6. Right to Information Act, 2009
7. Consumer Rights Protection Act, 2009
8. Contempt of Courts Act, 1926
9. Official Secrets Act, 1923
10. Copyright Act, 2023
11. Trademark Act, 2009
12. Patents and Designs Act, 1911
13. Children Act, 2013
14. Mobile Court Act, 2009
15. Bangladesh News Agency Act, 2018
16. Press Council Act, 1974
17. Cinematograph Act, 1918
18. Censorship of Films Act, 1963
19. Printing Presses and Publications (Declaration and Registration) Act, 1973
20. Note-Books (Prohibition) Act, 1980
21. Cable Television Network Management Act, 2006
22. Smoking and Tobacco Products Usage (Control) Act, 2005
23. Drugs and Cosmetics Act, 2023
24. Narcotics Control Act, 2018
25. Representation of the People Order, 1972
26. Code of Criminal Procedure, 1898

Internet Shutdowns and Infrastructure Control

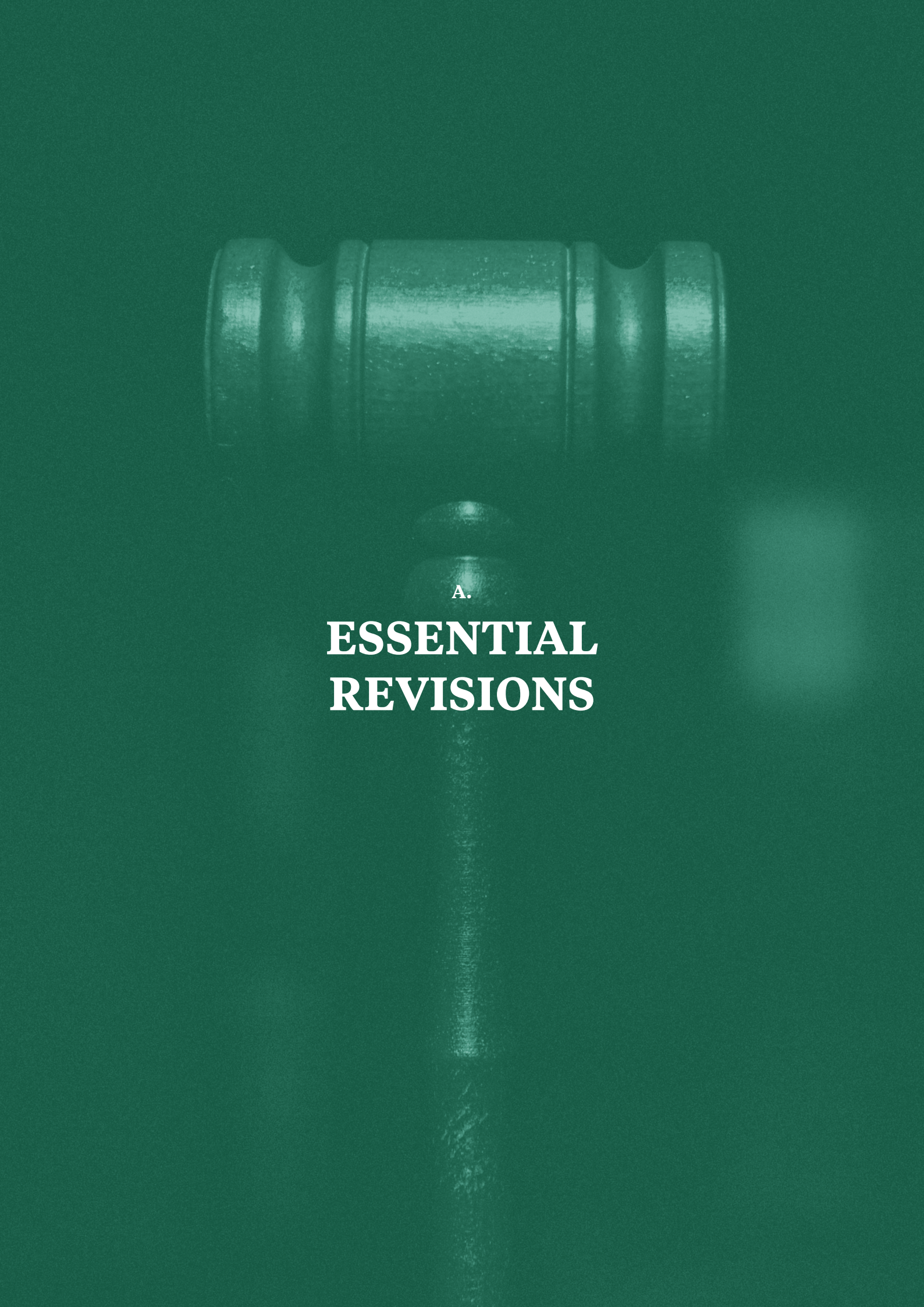
1. Bangladesh Telecommunications Regulation Act, 2001
2. Code of Criminal Procedure, 1898

Market Dominance

1. Bangladesh Telecommunications Regulation Act, 2001
2. Competition Act, 2012
3. Securities and Exchange Ordinance, 1969
4. Foreign Exchange Regulation Act, 1947

Search and Seizure

1. Part III, Constitution
2. Code of Criminal Procedure, 1898
3. Bangladesh Telecommunications Regulation Act, 2001
4. Special Powers Act, 1974
5. Narcotics Control Act, 2018
6. Anti-Terrorism Act, 2009
7. Money Laundering Prevention Act, 2012
8. Prevention of Corruption Act, 1947
9. Cyber Security Act, 2023
10. Information and Communication Technology (ICT) Act, 2006
11. Customs Act, 1969
12. Mobile Court Act, 2009
13. Explosives Act, 1884
14. Foreign Donations (Voluntary Activities) Regulation Act, 2016
15. Foreign Exchange Regulation Act, 1947
16. Bankers' Books Evidence Act, 2021
17. Statistics Act, 2013
18. Pornography Control Act, 2012
19. Consumer Rights Protection Act, 2009
20. Copyright Act, 2023
21. Patents and Designs Act, 1911
22. Imports and Exports (Control) Act, 1950
23. Special Powers Act, 1974
24. Censorship of Films Act, 1963
25. Note-Books (Prohibition) Act, 1980
26. Smoking and Tobacco Products Usage (Control) Act, 2005
27. Drugs and Cosmetics Act, 2023
28. Narcotics Control Act, 2018
29. Arms Act, 1878
30. Forest Act, 1927
31. Environment Conservation Act, 1995



A.

ESSENTIAL REVISIONS

1. Penal Code, 1860

SPEECH-RELATED OFFENCES

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 infringes upon fundamental rights to freedom of speech and expression, 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 and constitutional standpoint, these provisions use overly 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. Especially in online contexts, risks of misinterpretation and abuse are significantly increased.

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 the induction or attempted induction of students into 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, creating ambiguity about what constitutes unlawful political activity.

A low threshold for criminal liability—where even an attempt to induce political activity can lead to imprisonment—exacerbates the concern, as it allows for pre-

emptive and punitive actions against individuals or groups based on subjective interpretations of their intentions or actions. Constitutionally, the provision infringes on the rights to freedom of speech, assembly, association, and equality and non-discrimination, and safeguards against unlawful arrests and detentions.

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—this provision is in direct conflict with the constitutional pledges of a democratic society where political, economic, and social equality and justice is secured for all citizens. However, more problematically, the policy rationale behind criminalizing induction of students into politics, while simultaneously not disallowing students to engage in political activity and discourses, is inherently contradictory, since, if students are permitted to participate in political activities and discourses, banning their induction into politics serves no logical objective and undermines democratic participation.

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

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 contradicts the "*fundamental aim of the State 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*"—as enshrined in the Constitution. Overbroad, undefined, and vague elements of offenses, coupled with disproportionate penalties, is not only out of step with commitment to democratic

governance and fundamental rights but also fails to meet the requirement of legal certainty, necessity, and proportionality, under both the Constitution and international commitments.

Globally, many countries have moved to decriminalize or narrow the scope of 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 focused on strengthening offenses related to terrorism and hate speech. Other countries, such as India and Australia, have addressed criticism against the sedition provisions by altering the nomenclatures while keeping the substantive sedition and sovereignty provisions intact (see the *Bharatiya Nyaya Sanhita, 2023* and the *National Security Legislation Amendment Act 2010*), and are poor examples to follow.

Furthermore, Ireland, Denmark, Iceland, and Canada decriminalized blasphemy (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 of such provisions is significantly narrower compared to those in Bangladesh. For example, in the United Kingdom, incitement to certain offenses, such as hatred based on race, religion, and sexual orientation, is criminalized, but the provisions and the sanctions are narrowly tailored, and sufficient procedural guardrails 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). An offense of incitement to racial hatred requires an act to be threatening, abusive or insulting, and it has to be intended to or likely in all the circumstances to stir up racial hatred. However, in deciding on the public interest of charging the accused, 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. Secondly, 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, like South Korea, have multiple laws that restrict certain political activities, such as those involving activities related to national security or pro-North Korea ideologies,

those are narrow in scope and do not impose a broad ban 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—imposing an outright ban on student induction in politics, creates a constitutional conundrum: it does not disallow students to engage in political activity and discourses, merely their induction into politics, which is not only an unreasonable restriction on freedom of expression, assembly, and association, but also nearly impossible to enforce.

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 the speech criminalization under the defamation provision. Exceptions such as the imputation of truth for public good or the conduct of public servants are narrowly construed and subject to variable judicial interpretation, and, therefore, does little to mitigate the overarching threat to the constitutional right.

Even the penalty regime, entailing imprisonment for up to two years and/or unspecified amounts in fines, are disproportionately harsh; it can have a chilling effect on free speech and the free flow of information, deterring individuals—from ordinary citizens, journalists, and intellectuals to political oppositions and activists—from speaking out on matters of public interest for fear of legal retribution, leading to a less informed and less engaged citizenry.

Criminal defamation regimes are outdated and do not reflect the evolving nature of communication in the digital age: while the rapid dissemination of information is crucial for democratic participation and accountability, the speed and reach of digital platforms also increases the potential for defamation claims. This not only undermines the role of the internet as a platform for open and democratic discourse but also exposes individuals to significant legal risks simply for exercising their right to free expression. 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 considered inconsistent with international human rights standards, with many countries favoring civil remedies over criminal sanctions.

RECOMMENDATIONS

Delete the provision.

Delete criminal 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 decriminalize defamation and instead favor 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). Civil remedies, such as compensation for damages, allow for proportional responses, and more room for balanced adjudication through compensatory remedies and the rectification of reputational harm, without infringing on the fundamental right to free expression.

Section 509—Insulting women's modesty

ASSESSMENT

While the intent underscoring this provision is rooted in a legitimate desire to protect women from harassment and safeguarding their dignity, undefined and vague terms like "modesty" and "insult" and its construction within the nineteenth-century colonial governance structures makes it obsolete. At the time of its enactment, the deeply patriarchal Victorian ideals and socio-political constructs perceived women as the primary—and often only—group vulnerable to harassment, reinforcing the notion that women required paternalistic protection while men did not face similar threats, and reflecting limited understanding of vulnerability and gender roles. Similarly, the concept of "modesty" is a relic of colonial-era morality, reflecting rigid, patriarchal views of how women should behave and be perceived in society, based on the belief that women's virtue and dignity needed to be policed and protected.

Furthermore, these terms also attract subjective interpretation by law enforcement and the judiciary, which undermines the principle of legal certainty. From a social perspective, considering interactions in online spaces tend to be more casual and diverse, the ambiguous nature of the wording can be used to target and suppress voices online. Moreover, its broad scope could be used to rationalize policing and questioning women's interactions and behaviors, as well as to reinforce patriarchal norms and gender stereotypes, and restrict individual freedom, in the twenty-first century. This could also have the unintended consequences of deterring women from participating in online discussions or expressing themselves freely due to fear of legal repercussions.

A vague provision focused on "modesty" is insufficient to address the wide-ranging nature of modern harassment, which increasingly takes place in both offline and online spaces, and affects diverse groups beyond women. Further, rather than relying on vague and outdated concepts of modesty, there should be robust and context-sensitive laws specifically addressing harassment, stalking, and violence against women (and other vulnerable groups, such as transgender and intersex individuals, and minorities) in a clear and effective manner.

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

Enact standalone, gender-neutral, inclusive legislation against online and offline abuses.

Attempts to revise a single colonial-era provision will not serve the broader policy objectives of extending protection to those most susceptible to harassment, thus necessitating enactment of a standalone, comprehensive statute that addresses harassment in all its forms, aligned with the principles of human dignity, gender equality, and human rights.

Unlike the current legal framework in Bangladesh—including the amendments to the labor rules, 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*—which are inadequate to encompass and address harassment and abuses of different forms and in different medium, the proposed statutory enactment should afford universal protection against abuses 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 and gender identity.

Such legislation should avoid vague, subjective terms that can lead to arbitrary enforcement, and instead be focused on clearly defining different forms of abusive behavior, and specifically in online contexts, such as cyberstalking, cyberbullying, doxxing, trolling, catfishing, sextortion, flaming, cyber grooming, identity theft, hacking, revenge porn, online hate speech, defamation, media manipulation, and other forms of technology-facilitated abuses. As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has affirmed, and the Human Rights Council echoed, individuals' rights must be afforded equal protection online and offline, and that states have a duty to legislate to protect individuals from abuse in the digital realm (see A/HRC/38/35 and Resolution 38/7).

Section 294A (and the other statutes)—Gambling

ASSESSMENT

Existing legal framework on gambling—spanning multiple legislations, including the *Penal Code, 1860*, the *Public Gambling Act, 1867*, and the metropolitan statutes[1]—covers a range of activities, such as lotteries and betting, terms that have outdated and vague definitions. Furthermore, the statute prohibits gambling in "common gaming-house" using "instruments of gaming" does not logically extend to digital platforms, which are now the primary mediums for gambling.

While the courts in *Jafar Ullah vs Bangladesh* and *Mohammad Samiul Huq vs Bangladesh* have attempted to refine and clarify the statutory remit, there is no explicit guidance on whether these laws should extend to online lotteries and gambling, or other gaming services. Furthermore, although the Constitution mandates the state to prevent gambling, the legal framework is not sufficiently clear and comprehensive to meet this constitutional obligation offline, let alone online. Outdated and vague definitions of the provision means that the realities of modern gambling within the digital economy, which can be far more pervasive and accessible due to its cross-border nature, and associated financial loss, addiction, and other societal harms, remains unaddressed. Absent explicit provisions against online gambling, these services have flourished, often targeting vulnerable individuals, including minors, with minimal regulatory oversight.

Despite lack of specific legal provisions on online gambling, the authorities issue ad-hoc removal requests to offshore platforms like Google in respect of mobile applications in Google Play or content on YouTube, as well as user-generated content hosts like Facebook, Instagram, and TikTok. This raises concerns about due process, as individuals and businesses cannot be reasonably expected to comply with laws that are not clearly defined, and the vague terms could lead to arbitrary enforcement, making these removal orders susceptible to constitutional challenges for violating the right to protection of law and equality before the law.

1 For instance, the Rangpur Metropolitan Police Act, 2018, the Barisal Metropolitan Police Act, 2009, the Sylhet Metropolitan Police Act, 2009, the Khulna Metropolitan Police Ordinance, 1985, the Chittagong Metropolitan Police Ordinance, 1978, and the Dhaka Metropolitan Police Ordinance, 1976 each restrict gambling in public places.

Delete the provisions and the gambling law, and enact a well-structured, standalone statute.

Repeal archaic laws and scattered legal provisions.

Outdated colonial-era gambling laws—such as the *Public Gambling Act, 1867*—and scattered legal provisions on gambling in the *Penal Code, 1860* and the metropolitan statutes, should be repealed in its entirety. A consolidated and comprehensive standalone legal framework that clearly defines what constitutes gambling, both offline and online, and the circumstances in which it is considered an offense, should be enacted instead.

Countries worldwide have either banned, or heavily regulated, gambling in both online and offline space, with strict monitoring and enforcement mechanisms of both gambling activities and associated advertisements and financial transactions (see, for instance, Singapore's *Remote Gambling Act 2014* and Australia's *Interactive Gambling Act, 2001* and the *Interactive Gambling Industry Code* for effective laws on online gambling). Both laws disallow offshore operators to offer online gambling services to their residents, with state apparatuses actively blocking access to unauthorized websites and applications and imposing fines on companies that violate the law, as well as monitoring and sanctioning individuals who use unauthorized websites.

Clearly define the ambit, sanctions, and enforcement mechanism.

Given the constitutional requirement to restrict gambling, the proposed legislation must address the modern realities of gambling, particularly in the digital space, by providing clear guidelines and robust regulatory mechanisms. It should explicitly define various forms of gambling—including online betting, lotteries, roulette, poker, virtual slots, and any game of chance, including games of mixed chance and skill played over the internet, accessible within Bangladesh—to eliminate ambiguity and ensure clear distinctions between legal and illegal activities, and the scope of its application. If the law seeks to create exemptions, such as for licensed gambling operators, the statute should clearly articulate what activities constitute lawful and unlawful behavior.

Furthermore, since online platforms are now the primary medium for gambling, the law should explicitly define, and attribute penalties for, different categories of platforms based on their differentiated and contextual techno-commercial models (e.g., user-generated content services like Facebook, Instagram, TikTok, and YouTube, or mobile application stores operated by Alphabet and Apple, or search engines like Google or Bing—each serving as intermediary platforms for third-party content, mobile applications, or websites—are operationally and functionally different from one another, as well as from dedicated websites and applications for betting and gambling. Clear penalties, including fines and

imprisonment, should be defined for individuals and operators, and strictly enforced, based on their roles and responsibilities, and nature and extent of involvement, to deter unlawful practices.

A structured approach and effective regulation also necessitates establishment of provisions enabling regulatory monitoring and reporting of suspicious transactions and money laundering, and, where applicable, ensure proper taxation of gambling operators, as well as geo-blocking mechanisms and collaboration with international platforms (such as Google and Apple) to enforce compliance with local gambling laws. The existing ad-hoc approach to removal requests, as seen in the authorities' interactions with offshore platforms, lacks transparency and predictability, which opens the door to constitutional challenges on the grounds of violations of due process and equality before the law.

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). This may have been reasonable in the context of twentieth-century trade and societal norms: when the economy was predominantly physical and localized, the legal and regulatory oversight mechanisms to address unscrupulous business practices were rudimentary, and such practices were seen as mechanisms to manipulate consumers, drawing them into potentially fraudulent or exploitative commercial schemes. However, such incentive structures are common and legitimate commercial practices in today's digital economy to attract and retain customer engagement and loyalty. Hence, the provision not only creates a hostile environment for innovation and entrepreneurship but also undermines the government's broader policy objectives of promoting digital transformation and economic development.

For instance, promotional deals such as discount codes, cashback offers, and loyalty programs used by e-commerce platforms like *Daraz* or *Foodpanda*, or in-game rewards, prizes, virtual currencies, or other digital items offered in gaming applications such as *Fortnite* and *PUBG*, or offers of discounts and rewards on social media like Instagram and Facebook to users participating in challenges or engaging with content in brand-sponsored contests—each critical part of the business strategy and crucial for user engagement and retention—are unlawful under this provision. It creates a social disconnect between outdated legal norms and the current

realities of market behavior, potentially leading to widespread non-compliance. Constitutionally, the vague language and broad applicability of the provision creates room for arbitrary interpretation and enforcement, infringing principles of legal certainty and due process, as businesses cannot reasonably be expected to comply with laws that are no longer relevant or clear in their intent, as well as equality and equal legal protection guarantee and freedom of trade, business, and profession.

RECOMMENDATIONS

Delete the provision.

Decriminalize legitimate commercial practices, strengthen existing consumer and financial crimes laws.

As an archaic provision criminalizing commonplace, legitimate, and essential commercial practices—clearly misaligned with the modern economic and legal frameworks—should be repealed. 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. Thus, the legal focus should shift to 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. Other statutes are well-suited to address these concerns.

2. Pornography Control Act, 2012

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 terms like "sexually suggestive" and "obscene" content, and ambiguous terms like "semi-nude" and "sexually arousing" materials—risks 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 as binary. The definition not only infringes free speech and expression rights 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 on artistic and educational works (and on religious materials in section 9) is narrow and does 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 the work falls within the prohibited categories, as well as for individuals challenging conventional social norms or exploring themes related to sexuality, gender, or identity—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, and interactive platforms, with algorithms shaping access to pornographic material, 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.

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, 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 and 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 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 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, 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, 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, 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, in any medium, that depicts or describes, of or related to a person, any real or simulated sexually explicit acts, or any sexual organs, or any sexual exploitation or abuse, or any sexual services, where one or more depicted person has not given clear, informed, and voluntary consent for recording, production, possession, marketing, dissemination, purchase, sale, and display of each such material, 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, and 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 their sexual organs, or any sexual exploitation or abuse against or involving them, where one or more depicted person has not given clear, informed, and voluntary consent for the creation of each 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, 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.

OFFENCES

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 the 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, treating all sexually explicit materials as inherently damaging, also overlooks the need to address specific online harms. Moreover, the (over-)criminalization ignores the evolving societal norms where discussions around sexual autonomy and responsible consumption of adult content are becoming more accepted. 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 is a state overreach into private affairs that can be seen as a violation of the right to privacy and to access information, as well as infringement of a legitimate expression of personal freedom. Given the broad search and seizure mandate of LEA under section 6, and 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 potential exposure of the private, intimate behavior between consenting adults to public scrutiny, in addition to criminal liability—creating avenues for invasive state surveillance and punitive measure against individuals for personal or political reasons.

Furthermore, the abetment provision in section 8(7)—which attributes liability and punishment for 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 offenders' 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. 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 extraterritorial reach, 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 network level, reportedly in the tens of thousands, has 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.

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.

Additionally, 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; on the contrary, the statute mandates punishment the same rigorous imprisonment of up to seven years applies to both the production of pornography and the coercion of individuals into participating, despite the vastly different degrees of harm involved.

Over-criminalization erodes respect for the legal system and causes widespread non-compliance and underreporting, and risks driving harmful activities 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.

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 deep fake 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.

3. Competition Act, 2012

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. As a result, it remains unclear whether the statute is enforceable on offshore companies providing services to users in Bangladesh on a cross-border basis. Although there is a general presumption against extraterritoriality of statutes, a creative interpretation could extend the statute's reach to non-resident entities based on the location of the service recipient. 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 *Digital Markets Act* and Article 3 of the *General Data Protection Act* in the European Union). 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 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 definition of markets fails to account for the global nature of digital platforms, and could lead to incorrect assessments of abusive practices.

Outdated regulatory frameworks that do not reflect the realities of online

markets, where myriads of factors beyond price and characteristics, such as data, network effects, and platform economics, influence consumer decisions and competition in the markets for social media and online advertisements. For example, a social media platform's market power is not derived from its product characteristics or price, but rather from its user base, data collection and combination capabilities, and ability to leverage network effects to attract advertisers and outcompete rivals. The failure to include these considerations in the definition of relevant market could result in ineffective regulation that either fails to curb anti-competitive practices or stifles competition by misidentifying market power. Furthermore, competition in the digital marketplace is rarely homogeneous, even within a single country, due to factors such as varying levels of internet penetration, digital literacy, and local consumer preferences.

RECOMMENDATIONS

Amend the definition.

Expand the definition.

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 definition should be flexible and adaptive enough to acknowledge the heterogeneity of competition across regions by incorporating factors like local internet penetration, digital literacy, and consumer behavior into the regulatory framework, allowing for nuanced assessments in a shifting boundaries of markets and competition.

Furthermore, the definition should account for abuses across multiple 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).

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 is in its current form not fit for the digital ecosystem and unique characteristics of the digital services. Online intermediaries, like Facebook and YouTube, offer services without charging the users, instead collecting user data and leveraging user attention to serve as the currency—the value exchange in digital transactions and interactions does not always align with traditional commercial models. Without a clear and precise legal framework, there is a risk of regulatory gaps or overreach, which could lead to inconsistent enforcement.

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). Due to the incomplete definition, it is unclear to determine the threshold at which a service is subject to regulation, particularly in cases where the services are provided without financial consideration.

RECOMMENDATIONS

Amend the definition.

Expand the definition.

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 *Digital Markets Act* in the European Union). A clear threshold should be set to objectively assess whether a service is subject to regulation, even if no financial consideration is involved, ensuring clarity on the regulatory obligations of platforms. For additional clarity, the definition, and overall framework of the statute, should be revised to recognize and regulate services operating on cross-side and multi-side business models (e.g., connecting advertisers, users, and content creators), where the value of the service is derived from interactions between different user groups and market dynamics differ significantly from traditional one-sided markets.

ANTI-COMPETITIVE BEHAVIOUR

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 somewhat rigid definitions do adequately not 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. This could lead to service providers being wrongly classified as anti-competitive or, conversely, escaping necessary scrutiny.

The threshold for what constitutes "abuse of dominant position" or "anti-competitive behavior" remains ill-defined within the context of digital markets. 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. However, such interpretation could unintentionally stifle innovation, hinder market access, and fail to protect consumers.

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. GAFAM companies like Alphabet and Meta offer free services but collect vast amounts of user data, which they monetise through targeted advertising, and the lack of recognition of data as a valuable commodity means that such platforms could evade scrutiny despite engaging in anti-competitive behavior. Illustratively, the provisions fail to address click-through user agreements, which are commonly used by digital platforms to bundle unrelated services, such as requiring users to accept conditions that grant access to personal data or prevent users from utilizing competing services, which can amount to anti-competitive behavior. Facebook conditions access to its social media platform on users granting permission for their data to be scraped from third-party sites and shared with its affiliated companies, thus strengthening its

dominance in digital advertising—and this was sanctioned by German competition authority, and Meta was prohibited from engaging in such abusive commercial practices.

Certain provisions related to abuse of dominant positions, specifically section 16(2)(c), (d), and (e), are sufficiently broad in their language to encompass a wide range of activities by, for instance, GAFAM companies. At least in theory, these provisions could sanction companies for engaging in anti-competitive practices, such as restricting market access for new or smaller firms through restrictive data practises and or self-preferential behavior, or compelling market actors and consumers to enter into contractual arrangements with collateral obligations like making services accessible conditional on giving unlimited access to personal data or on acceptance of other services (such as cloud storage, or advertising tools, or payment gateways), or leveraging dominance in one market to gain an advantage in another market.

For instance, Google could use its market power in the search engine market to push streaming services, and Amazon could use third-party seller data to develop competing private-label products. However, despite this breadth, the provisions are not sufficiently nuanced to fully address intricacies of competition in the digital marketplace—unique characteristics such as network effects, data collection and combination, and algorithms can create "walled gardens" that restrict consumer choice and adversely impact market competition.

RECOMMENDATIONS

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

Set clear digital-specific thresholds for abuse of dominance.

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 (see section 18 of the *German Competition Act*). An effective regulation is conditional on recognition that data is a commodity in anti-competitive assessments, and implementing data-centric regulatory measures and metrics that focus on the volume, type, and usage of collected data as factors as part of the competitive analysis and for determining regulatory oversight.

Equally important is to clarify that certain provisions, such as those on predatory pricing in digital context, where offering services for free or at low cost is a legitimate business model, is not sanctioned (see reports by the Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary of the U.S. House of Representative on Competition in Digital

Markets and 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).

Expand the remit of anti-competitive behavior.

Identify and incorporate new categories of anti-competitive behavior. Certain exclusionary and anti-competitive practices should be expressly treated as anti-competitive behaviors, including, for instance:

systemic monopolistic behavior by Alphabet in the search engine and advertising technology markets, and using search dominance to promote its own services, such as streaming platforms or cloud services or shopping results (see *United States v. Google LLC* (2020) and *United States v. Google LLC* (2023), and the investigation report of the Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary of the U.S. House of Representative on Competition in Digital Markets (2020), in the United States; section 19a of the *German Competition Act* and *Alphabet Inc. v. Germany* in Germany).

abusing dominant position in the mobile application distribution market by Apple and Alphabet to compel developers to use their payment gateways (*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; and see section 50 of the *Telecommunications Business Act* in South Korea).

exclusionary conduct by Apple, developing its products to limit third party digital wallets, smartwatches, and messaging on its devices (see *United States v. Apple Inc.*).

collusive arrangements between Apple and Google, and device manufacturers and carriers, that sets Google as the default search engines in Safari and Chrome browser (*United States v. Google LLC* in the United States; see also Digital Platform Services Inquiry – September 2024 report revisiting general search services in Australia).

using abusive acquisitions strategies and self-preferential algorithms, and engaging in exclusionary data practices and cross-market leveraging of user data to drive out competition, by Meta (see the settlement order between Meta and the Federal Trade Commission for US$ 5 billion 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).

abusing dominant position in the e-commerce markets by Amazon, using interlocking anticompetitive and unfair strategies—including using third-party seller data to create competing private-label products, manipulating price, and preventing rivals from fairly competing against Amazon (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).

Additionally, explicit language should be incorporated that prevents companies from using dominance in one area (e.g., search engines) to prioritize their own products or services (e.g., streaming services or e-commerce), and from creating "walled gardens" through data monopolization and user lock-in strategies.

Regulation of click-through 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 (see, for instance, *Meta v. Bundeskartellamt* Case C-252/21, and *Bundeskartellamt v. Google* and *Bundeskartellamt v. Meta* in Germany; also, the bundling of user consent choices in a single button for general terms and conditions, privacy policy, cookie policy was deemed unlawful in *Douglas Italia*).

ORGANIZATIONAL STRUCTURE

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

ASSESSMENT

This provision fails to account for the highly technical and niche nature of the digital market, making the Competition Commission an ineffective tool for regulating competition in this space. Current framing of experiences in broad areas such as economics, market matters, public administration, or law does not ensure that the members of Competition Commission possess the specific expertise needed to understand and address factors impacting competition in digital markets, such algorithms, data-driven business models, and the rapid pace of technological change. Without such expertise, the Competition Commission risks being a blunt instrument, unable to effectively distinguish between competitive innovation and anti-competitive behavior. This could lead to either over-regulation, stifling innovation and market growth, or under-regulation, allowing harmful monopolistic practices to flourish unchecked.

Amend the organizational structure of the Competition Commission.

Mandate 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 can be achieved by creating a specialized digital markets unit within the Competition Commission focused on digital competition issues, staffed with experts. Additionally, the statute should enable the Competition Commission and its specialized unit to consult external technical experts in data science, software engineering, and other relevant digital disciplines when assessing anti-competitive behavior in digital markets.

Amend the statute to mandate ongoing training for members of the Competition Commission on emerging technologies, digital business models, and global regulatory practices in the digital space. Furthermore, clear provisions should be incorporated to establish formal mechanisms for regular dialogue between the Competition Commission and key digital market stakeholders, including tech companies, civil society, offshore regulators, and academics. This would facilitate informed decision-making and encourage collaboration in crafting fair and effective digital market regulations

Finally, empower the Competition Commission to create issue-specific guidelines that outline how the agency will assess digital market practices, including issues like self-preferencing, network effects, algorithmic transparency, and data monopolization, without having to amend the statute frequently. These amendments would ensure the Commission is capable of understanding and regulating the complexities of digital ecosystems.

4. Consumer Rights Protection Act, 2009

SCOPE AND APPLICATION

Section 1—Application of the law

ASSESSMENT

The statute does not specify the scope and application, meaning while it would apply to enterprises operating within the country, it may not have extraterritorial application and may not be enforceable on offshore companies providing services to users in Bangladesh on a cross-border basis.

RECOMMENDATIONS

Amend the scope and application.

Extend the statute's jurisdiction to include extraterritorial applicability.

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 the *Fair Trading Act 1986* in New Zealand and section 5(8) of *Consumer Protection Act, 2008* of South Africa; see also, for instance, Article 1(2) of the *Digital Markets Act* and Article 3 of the *General Data Protection Act* in the European Union). This would ensure that GAFAM companies offering cross-border services are subject to Bangladeshi consumer protection regulations. To avoid overreach, the statute should include clear application criteria, for instance, based on user base size or revenue generated from the country (see Article 3 of the *Digital Markets Act* in the European Union and section 1798.140(d) of the *California Consumer Privacy Act of 2018*).

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. While the current definition could work for e-commerce platforms like *Daraz* or *Foodpanda*, the definition fails to capture the essence of digital transactions on social media, search engines, and other "free" online services, where users, in exchange for access to platforms, provide personal data that technology companies monetise—a techno-commercial model that is intrinsically different from the conventional consumer transactions envisioned by the current legal definitions. A failure to consider the nuances of data as a form of consideration raises concerns around privacy and data protection; consumers are vulnerable to exploitation, as their data could be used in ways they did not anticipate or consent to, without the legal recourse typically available in traditional consumer transactions.

Furthermore, as currently framed, the definitions in sections 2(3) and 2(19) are not fit-for-purpose in the rapidly evolving digital landscape, where consumers, advertisers, and service providers interact in ways that the existing legal frameworks were not designed to regulate, leaving consumers in the digital economy unprotected.

Moreover, the mandate of the DG-DNCRP in section 21, and the overall architecture of the legislation, reflects a conventional understanding of commerce, where consumer protection is primarily concerned with the quality and safety of physical goods and the integrity of face-to-face transactions, indicating legislative intent to regulate traditional businesses. Consumer harms in the online marketplace arise not only from the quality of physical goods, but from practices such as data exploitation, algorithmic bias, or unfair competition, issues not addressed in this statute.

RECOMMENDATIONS

Amend the definition and regulatory mandate.

Expand the definition and scope of consumer harms.

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. This would recognize users of "free" services like social media platforms as consumers entitled to legal protections. Alternatively, adopt a neutral definition that does not require exchange of consideration (see, for instance, Article 3(c) of the *Digital Services Act* in the European Union).

Concurrently, the statute needs to be amended to establish explicit data-related legal protections that safeguards consumers from data exploitation, such as unauthorized data sharing or use beyond the user's consent, while expanding protection to cover non-traditional harms, such as algorithmic bias, data exploitation, or predatory data practices (see Articles 5 and 6 of the *Digital Markets Act*, Articles 34 and 35 of the *Digital Services Act*, and Articles 5 and 22 of the *General Data Protection Act* in the European Union; see also the draft automated decision making technology regulations in the United States). This would help protect users of digital services from opaque data usage practices by platforms and offer recourse in case of privacy violations or data misuse.

Section 2(22)—Definition of "service"

ASSESSMENT

Definition of "service" as provided in the current provision is overly narrow and prescriptive, limited to services to traditional utilities and sectors like transport, telecommunication, and healthcare, and specifically excluding those provided free of charge. By expressly excluding services that are offered without direct financial remuneration, the provision fails to account for the full spectrum of activities that constitute services in the digital economy, and to provide a legal framework to regulate these significant and pervasive services, leaving a large portion of the digital economy outside the scope of consumer protection laws. Additionally, it also disregards the broader implications of data exploitation, privacy concerns, the influence of

digital platforms on public discourse and behavior, and other anti-consumer tendencies of technology companies. The current threshold for what constitutes a service, tied to the exchange of consideration, is an outdated concept in the context of the digital economy.

RECOMMENDATIONS

Amend the definition.

Expand the definition.

Broaden the definition of "service" to include non-remunerated services that are characteristic of many online services, which relies on data or user attention. Specifically and explicitly include data-driven services, social media platforms, search engines, and other digital services that significantly impact users' rights, behaviors, and choices (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 *Digital Markets Act* in the European Union). This would ensure that companies offering "free" digital services are subject to consumer protection laws.

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

ASSESSMENT

Coupled with the restrictive definition of "service," the narrow and prescriptive definition of the term "anti-consumer right practice" in section 2(20) fails to address diverse and sophisticated forms of consumer harm that can occur in the digital marketplace. Furthermore, the focus of the definition on traditional goods and services, such as false advertisement or failure to deliver services under sections 2(20)(d), 2(20)(e), 44, and 45, which, while important, are rooted in traditional notions of consumer protection and do not capture the nuances of online transactions.

For example, in e-commerce, consumers may face issues such as the manipulation

of search algorithms to prioritize certain products, deceptive pricing practices that exploit personal data, the bundling of services in a way that misleads consumers, or the use of dark patterns to influence consumer behavior. Practices such as data mining, targeted advertising, and the creation of filter bubbles can significantly impact consumers' autonomy, privacy, and even mental health, yet these issues are not addressed under the current legal framework. A failure to account for these more complex forms of digital deception, and insular focus on traditional, one-dimensional service transactions, leaves consumers vulnerable to exploitation and without constitutional right to redress. Further, the non-inclusive provisions could lead to unequal treatment of consumers depending on whether the transaction is conducted using traditional avenues or digitally, potentially contravening constitutional principles of fairness and equality.

RECOMMENDATIONS

Amend the definition.

Expand the definition.

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 harmful behaviors should be expressly treated as anti-consumer right practice, including, for instance:

using personal data and bundling services to create discriminatory pricing models (see disclosure orders issued to eight companies for surveillance pricing, and Orbitz using steering strategies to advertise expensive hotels to consumers of Apple products, in the United States).

non-transparent use of algorithms, particularly in search rankings or recommendation systems, that enables manipulation and self-preferential treatment towards certain products or services (see, for instance, *Google v. Germany*, and complaint filed against Temu and decision against Amazon in the European Union).

collecting extensive amounts of personal and non-personal data from users on the basis of click-through agreement, and often without consent, for product and services improvement, pricing adjustments, and advertisement (*Meta v. Bundeskartellamt*; *Bundeskartellamt v. Facebook* in the European Court; see, in relation to the Cambridge Analytica scandal: (a) the settlement for US$100 million 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).

using dark patterns—that is, complicated and manipulative user-interface with skewed wording, confusing choices, repeated nudging, and misleading strategies and repeated misdirection—to make cancellation process difficult, or trick consumers into enrolling into subscriptions by Amazon (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 million).

Adoption of more robust consumer protection legislation will not only bring sophisticated forms of digital exploitation under regulatory oversight, it will also enable consumers to enjoy the same level of protection as those in traditional markets consistent with constitutional principles of fairness and equality. Additionally, the DNCRP should be empowered to create issue-specific guidelines to address emerging forms of anti-consumer rights practices in the digital ecosystem, without having to amend the statute frequently, exercising its delegated legislation authority and after conducting public consultations.

A. ESSENTIAL REVISIONS

5. Bangladesh Telecommunication Regulation Act, 2001

SCOPE AND APPLICATION, DEFINITIONS, AND ROLES AND RESPONSIBILITIES

Sections 2(11), 2(14), 3, 29, 30, 31, 35, 61, 63—Definitions of "telecommunication" and "telecommunication service," application of the law, and objectives, responsibilities and powers of BTRC

ASSESSMENT

Expansive definitions of certain terms—such as "telecommunication" defined in section 2(11) as including speeches, sounds, signs, signals, writings, visual representations, and other form of intellectual expressions, and "telecommunication service" defined in section 2(14) as including transmission and reception of telecommunication, value-added services, and internet services—when read with the broad roles and responsibilities of BTRC under sections 29 and 30, has led to an interpretation that online communication channels fall under the regulatory purview traditionally reserved for telecommunications. Specifically, the inclusion of internet services and value-added services under "telecommunication services" has been taken to mean that social media platforms, streaming services, and other online intermediaries are subject to the same regulatory framework as conventional telecommunication operators, despite these online services differing significantly from traditional telecommunication operations.

For instance, social media or online dating platforms, which operate on user-generated content and data-driven advertising models, are fundamentally different from streaming services, which serve curated (such as Netflix) or user-generated (such as YouTube) content. These services are operationally and functionally different from traditional telecommunication services that focus on the transmission of voice and data. Yet, section 35(1) mandates mandatory licensing for any entity providing "telecommunication service," else risk criminal and administrative penalties. As currently framed, it is unclear whether these distinct service providers, such as social media platforms and streaming services, should be classified as telecommunications service providers,

thereby requiring them to comply with licensing requirements.

Where the licensing requirements apply, the associated penalties—including administrative fines of BDT 3,000,000,000, with additional fine of BDT 10,000,000 for each day of non-compliance, and possible registration cancellation, under section 63—are unduly harsh.

Additionally, section 61 authorizes LEA to enter any premises at a reasonable time if there are reasonable grounds to believe that telecommunication services are being provided without the necessary license or in violation of its terms, and seize equipment, documents, or data, and extract information, or interrogate individuals, if necessary for the enforcement of the statute, without prior judicial warrant. Any obstruction or false information could attract a maximum of three years' imprisonment and/or administrative fine of BDT 1,000,000,000.

Altogether, the legal framework creates a disincentive for these offshore companies to establish offices and obtain registration in Bangladesh.

A linear, one-size-fits-all approach not only conflates traditional telecommunications with digital services that operate on fundamentally different principles, but it also overextends the jurisdiction of a statutory agency originally established to manage telecommunications infrastructure and services to regulate online intermediaries. This indicates a lack of understanding of the distinct economic models, operational structures, and regulatory needs of different online service providers.

By assuming roles outside its purview, the BTRC cannot effectively address online-specific concerns such as misinformation, cyberbullying, and data security, and this overextension raises constitutional concerns regarding overregulation and potential infringements on fundamental rights, including freedom of expression and privacy. Excessive government control over online information risks promoting monitoring and censorship on a scale inconsistent with democratic governance. Absence of clear mandate and express extraterritorial application of the statute raises questions about the regulatory authority exercised over foreign social intermediaries, such as Facebook, TikTok, and YouTube.

RECOMMENDATIONS

Additionally, clarify that the definition of "telecommunication service" in section 2(14)—and specific reference to internet service and value-added service—does not extend to online intermediary services. This will distinguish telecommunications infrastructure operators and service providers (such as mobile network operators, international internet gateway, and internet service providers) from digital platforms (such as online content providers, messaging applications, and cloud storage), reducing regulatory overreach over platforms that do not fit within the traditional telecommunications framework.

Define online intermediaries explicitly as a category in the amendment, distinguishing them from traditional telecommunication service providers (see, for instance, the definitions of 'core platform service' in the *Digital Markets Act* in the European Union). Clear definitions for social media, streaming, hosting, search, caching, content-sharing, and other intermediary services under that category would enable a regulatory approach that considers the unique operational and economic models of each service type, promoting targeted oversight without overreach. Specifically, clarify that the licensing requirements, revenue, tariff, and penalty regulations, originally designed for telecommunication services, are not applicable to online intermediaries. Each of these issues, where applicable, should be defined under digital-specific legislation and be proportionate to the nature of digital services, avoiding undue harshness that may deter business operations.

Redefine regulatory mandate and jurisdictional parameters.

Amend the roles and responsibilities of the BTRC under sections 29 and 30, and scope and application of the statute in section 3, to expand its jurisdiction to also include online platforms and technology and internet-enabled service providers. Of note, the Australian Communications and Media Authority, the Malaysian Communications and Multimedia Commission, the Infocomm Media Development Authority in Singapore, and the Ofcom in the United Kingdom each serves as "super regulator" with mandate over telecommunication, broadcasting, and/or online content—and the BTRC could similarly be structured. However, clarify that the proposed amendment, rather than regulating online intermediaries under the telecommunication laws, is aimed at empowering the BTRC to exercise oversight in specific circumstances (e.g., where authorized under the existing *Cyber Security Act, 2023* or the proposed *Online Safety Act* (see below)).

OFFENSES

Sections 66, 66A, 69—Content, signals, and calls that are false, anti-state, or obscene

ASSESSMENT

When BTRC applies these provisions to a platform like Facebook, WhatsApp, YouTube, and other online intermediaries, it stretches the statute's intended remit, which was originally designed for legacy telecommunication services. Under sections 66 and 66A, the transmission or facilitation of "signals," "messages" and "calls" that are false or fraudulent, or undermines national unity, security, public order, sovereignty, or create public fear or dissension, are criminal

offenses, punishable with five years' imprisonment and fines of up to BDT 3,000,000,000, with the added risk of service discontinuation for both offenders and the entities enabling the transmission. Similarly, section 69 criminalizes the transmission of obscene, offensive, threatening, or insulting content, imposing penalties of two years' imprisonment and fines up to BDT 5,000,000,000. These provisions, while initially intended for traditional telecommunication services, are now ambiguously and broadly applied to digital services, extending to platforms not originally meant to be regulated under the statute. This raises serious concerns regarding potential infringements on fundamental rights such as freedom of expression, privacy, and due process.

While the provisions aim to prevent harm like incitement to violence, hate speech, and fraud, they are not sufficiently tailored to the unique forms of online harm prevalent on social media platforms—such as misinformation, cyberbullying, or extremist content. Broad, punitive measures, including heavy fines and imprisonment, are blunt instruments that fail to address the root causes of these online harms or provide adequate safeguards for users' rights in the decentralized and dynamic context of the internet. Furthermore, the broad enforcement powers granted to BTRC, including the ability to block or seize communications without judicial oversight or the need to assign reasons, undermine due process protections and invite arbitrary use of power.

A significant policy challenge arises from applying telecommunications law to internet-based services, which operate under entirely different business and technical models. Notably, social media, streaming, and messaging platforms operating across borders, often without physical infrastructure in Bangladesh, makes enforcement under these provisions difficult. Additionally, these provisions overlook the operational nuances of these platforms, where intermediaries do not typically exercise direct control over user-generated content but may still be held liable. This misapplication of outdated telecommunication laws risks stifling innovation, limiting consumer choice, and hindering the development of local digital businesses, creating a regulatory environment that is incompatible with the needs of the modern digital economy.

RECOMMENDATIONS

Amend the statute as recommended above, and additionally limit liability of online intermediaries, and revise definitions and penalties.

Liability limitations for online intermediaries.

Amendment of the statutory scope and application as recommended above should limit the application of sections 66, 66A, and 69 to traditional telecommunication services. If the amendments are not enacted, modify the provisions to clarify that their

application is limited to traditional telecommunication services and exclude platforms that primarily function as intermediaries for user-generated content. Additionally, in the interest of completeness, a safe harbor provision could be introduced to protect online intermediaries who do not exercise direct control over user-generated content, limiting their liability for third-party content.

Define terms clearly, and delete provisions. Amend the provisions to provide clarification on what constitutes "signals" and clearly define the scope of what constitutes false and fraudulent content, as well as set clear threshold on actions undermining national unity, security, public order, sovereignty, or creating public fear or dissension, as these are open to multiple interpretation, and could, therefore, result in over-application of penalties. Ambiguous terms like "offensive," "threatening" and obscene should be deleted due to their inherently subjective nature.

Revise disproportionate penalties. Overbroad penalties—with non-cumulative fines ranging between BDT 3,000,000,000 and BDT 5,000,000,000 and harsh imprisonment terms—for offenses that are not necessarily serious in nature or effect, and susceptible to abuse due to its inherent vagueness, should be replaced with proportionate criminal fines and no incarceration.

INVESTIGATIVE POWERS

Sections 67, 71, 73—Unlawful interference and interception

ASSESSMENT

While the intent of these provisions is to criminalize unlawful interference and interception of communications, their ambiguous language and narrow scope fail to sufficiently cover modern forms of unlawful surveillance, particularly in the context of internet-based messaging and video calling applications. Specifically, section 71 is excessively narrow in scope, as it criminalizes only unauthorized interference by an individual with a conversation using legacy telecommunications networks, specifically exempting Intelligence Agencies and other LEAs. Similarly, wilful alteration or distortion, or interference with content of messages, is criminalized in section 73(1) only if the message is transmitted over legacy telecommunications networks.

From a legal and constitutional perspective, the vague and undefined language—like "wireless communication," "without lawful cause" and "interception"—lacks clarity and precision, while reference to transmission over telecommunications networks makes it difficult to ascertain its application to encrypted communications platforms such as WhatsApp or Zoom that uses internet services. Moreover, it is unclear whether the law covers, or adequately addresses, the complex, multilayered threats that modern internet-based communications face, such as man-in-the-middle attacks, tracking metadata, real-time monitoring of communications, and unauthorized state-sponsored surveillance, leaving gaps in its ability to effectively protect individuals' right to privacy and freedom of communication. A failure to account for the evolving nature and full spectrum of communication technology makes the law ineffective in addressing the realities of digital communication. This ambiguity creates the risk of uneven enforcement and could leave significant loopholes that may be exploited for unlawful surveillance or wiretapping.

Sections 97, 97A, 97C—Interception

ASSESSMENT

From a legal perspective, section 97 confers unfettered authority to state agencies over telecommunications operators and service providers during states of war, internal rebellion, or national security concerns, without any concrete legal standard for assessing the proportionality or necessity of these actions, with the power to authorize suspension, modification, and interception of services with minimal oversight and vague justifications. This provision effectively overrides other legal protections or rights, such as those related to the freedom of speech, privacy, and access to information, with no procedural safeguards, making this provision ripe for arbitrary and excessive enforcement. Furthermore, sections 97A and 97C expressly authorize Intelligence Agencies and other LEAs on national security or public order to carry out interception of private communications, as well as collect and record information, without sufficient judicial oversight, and service providers are mandatorily obligated to share information and extend assistance, else risk harsh fines and imprisonment.

Although the provision references national security and public order, the term is undefined, leaving room for subjective interpretation by the state agencies. Virtually any situation could be framed as a "public order" issue or a threat to "national security," where broad surveillance powers could be used to monitor and control online discourse under the guise of protecting national interests. Ordinary citizens' communications could be intercepted for reasons unrelated to any real or imminent threat, and lack of judicial oversight means that citizens have limited recourse to challenge such invasive state actions.

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 uncertainty and leaving service providers vulnerable to arbitrary and excessive demands for information.

Specifically sub-sections (1) and (3) of section 85 creates avenues for infringement of individuals' right to privacy under the Constitution and established principles of data protection rights, as it enables BTRC to publicly disclose information received during the course of investigation or proceedings, including sensitive data, trade secrets, proprietary technologies, intellectual properties, personal user data, and business information, with or without allowing data owner the opportunity to be heard. While there is a provision for a hearing before disclosing confidential information, broad discretion conferred to BTRC in determining what constitutes public interest means service providers are at the mercy of subjective regulatory decision-making, raising concerns about the adequacy of protection of sensitive or proprietary information. By relying on a framework intended for traditional telecommunication networks, they fail to address the nuanced operational models of digital platforms, including social media and streaming services, which may require a more tailored regulatory approach. Additionally, the absence of robust safeguards against unauthorized access to this information by third parties, or even insiders, heightens the risk of data breaches or misuse, which could have far-reaching consequences.

RECOMMENDATIONS for *Sections 67, 71, 73, 84, 85, 97, 97A, 97C*

Delete the provisions, and if not, amend and provide illustrations.

Clarify scope of unlawful interference and interception provision.

As currently framed, it is unclear whether criminalization of interference and interception extends to internet services, such as messaging applications (e.g., WhatsApp and Telegram) and video-conferencing services (e.g., Zoom and Teams), or only to communications over legacy telecommunication networks and systems. Amend the provision to clarify the scope of the statutory protection.

Delete surveillance and interception provisions.

The current legal framework on surveillance and interception—including provisions of the *Bangladesh Telecommunication Regulation Act, 2001* and other laws addressed in this paper—is fragmented and opaque, granting excessive discretionary powers to state agencies without meaningful judicial oversight. While necessary in a democratic society to combat threats, such as terrorism, cybercrime, and serious national security risks, these activities must be conducted under a clear and accountable legal regime. Deletion of existing surveillance

and interception provisions, and the enactment of a new statute designed to address the need for such activities while ensuring procedural safeguards, is critical. This statute should provide a streamlined and transparent approach to lawful surveillance and interception, under clear and established procedures that includes safeguards like prior judicial authorization, independent oversight mechanism to monitor compliance, structures that enable time-limited and scope-specific interference, and avenues for redress for individuals affected by unwarranted surveillance and interception. These measures must be proportionate and in compliance with constitutional requirements, particularly in a country where democratic institutions are still evolving, without infringing on fundamental rights.

Clarify terms and behaviors covered for completeness.

Assuming non-adoption of the recommendation for new statutory enactment, key terms like "interception" and "surveillance" should be defined, or adequately explained with illustrations similar to illustrative examples in the *Penal Code, 1860*, to clearly delineate the scope of its application. Likewise, terms like "national security" and "public order" should be clearly defined to limit the scope of state actions under these provisions, preventing vague justifications for surveillance or service suspension. Furthermore, the authority of the BTRC to request information from service providers should explicitly outline categories of information covered. Due to its inherently invasive nature, the provisions should be specific and unambiguous.

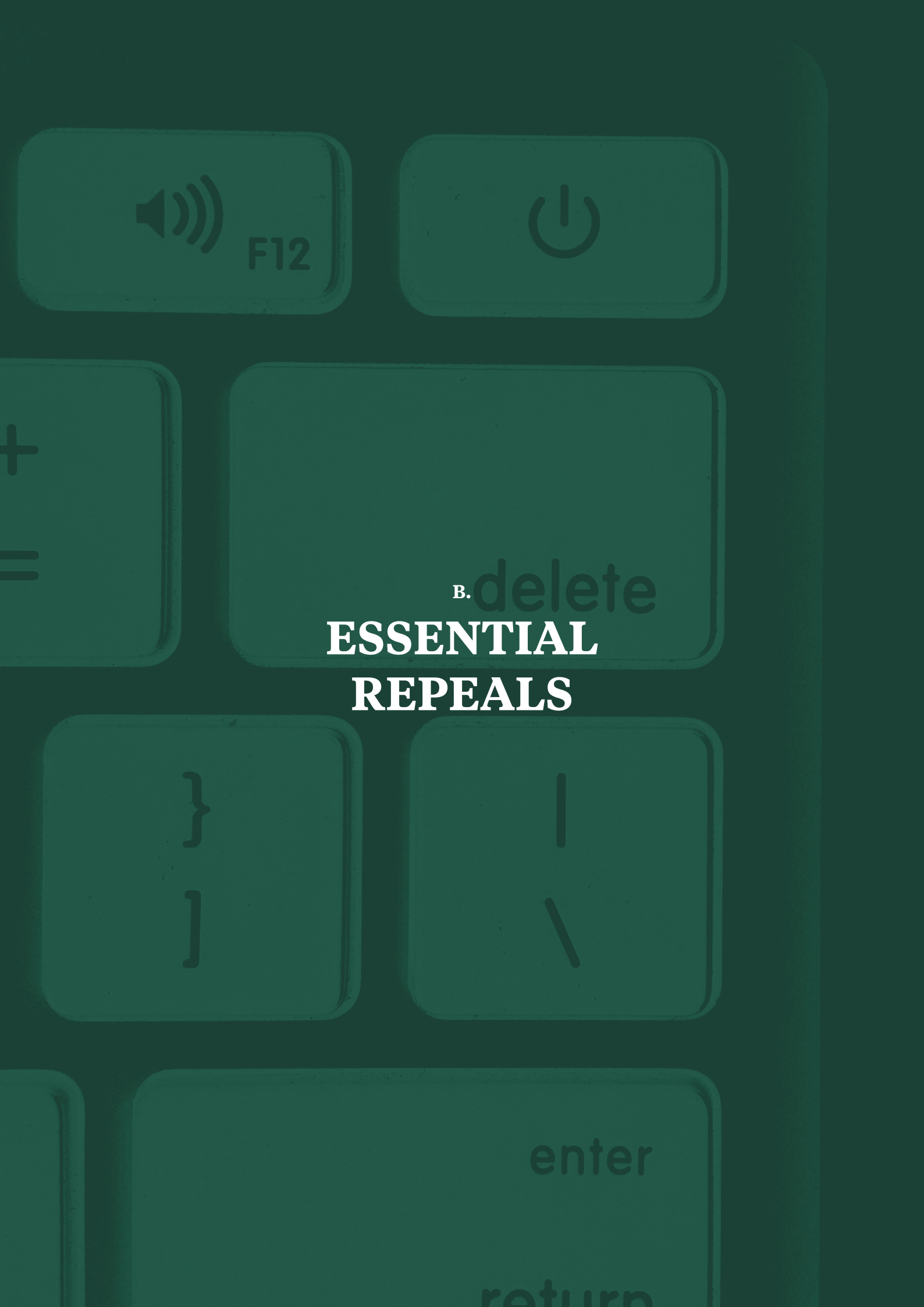
For instance, while section 97A presumably encompasses wiretapping over telecommunication networks, covert audio and video recording, geo-location tracking, and signal interception, it remains unclear whether it covers more sophisticated systems—like facial recognition systems, laser microphones, metadata collection, browser tracking and cookies, spoofing, man-in-the-middle attacks, keylogging, deep packet inspection, cell site simulators, phishing, scraping, browser fingerprinting—or lesser known methods like technology-enabled social engineering and content moderation and platform monitoring. Specifically, the provision should also clarify whether, if at all, interception and surveillance over internet-based messaging and video calling applications and social media are covered by the statute.

Clarify the scope of disclosure provision.

Overbroad authority of the BTRC to request information from service providers under section 84 should be guided by clear procedures, including criteria for necessity, transparency requirements, and mandatory judicial oversight, especially for sensitive or proprietary data.

Delete LEA information disclosure powers.

Deletion of sub-sections (1) and (3) of section 85 is critical to protect trade secrets and sensitive data. Additionally, the provision should impose specific obligations to ensure that information shared is securely handled and cannot be disclosed without a judicial or independent oversight process.



B.

ESSENTIAL REPEALS

Cyber Security Act, 2023

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

ORGANIZATIONAL STRUCTURE

Sections 5(3), 5(4), 7—Authorities, functions and responsibilities of NCSA to be prescribed by rules, and organizational structure subject to government approval, and *Section 12*—Composed exclusively of state actors, and operating under direction of the prime minister, NCSC includes members of the DGFI, NSI, NTMC, and Bangladesh Police.

ASSESSMENT

Despite its intended status as an independent statutory authority, the subordination of NCSA to a ministerial division raises concerns about its ability to protect citizens' rights and interests fairly and transparently, without undue government influence. Furthermore, leaving its authorities, functions, and responsibilities to be determined by rules risks creating a regulatory framework that is vague, inconsistent, and open to manipulation and politicization.

Autonomy and agency are necessary to fulfill statutory mandates and its overall legitimacy.

Composition of the NCSC raises concerns about the lack of diverse representation and inclusivity in cybersecurity governance, which can lead to groupthink, where decisions are made without sufficient debate or consideration of alternative perspectives. Absent independent experts, civil society representatives, legal scholars, industry representatives, and other private sector stakeholders, there are risks of narrow, security-focused approach at the expense of broader economic and civil liberties, potentially leading to a governance model that is reactive rather than proactive in addressing cybersecurity threats.

SPEECH-RELATED OFFENSES

Online speech criminalized under the statute includes:

(A) section 21—propaganda or campaign against

a. liberation war

b. spirit of liberation war

c. father of the nation

d. national anthem

e. national flag

(B) section 24—identity fraud and personation

(C) section 25(1)(a)—content offending, insulting, humiliating, maligning, annoying, or threatening a person

(D) section 25(1)(b)—content maligning the image or reputation of the country

(E) section 26—unauthorized collection, possession, sale, use, or transmission of identity information

(F) section 28—content hurting religious values or sentiment

(G) section 29—defamatory content

(H) section 31—content that

a. creates communal enmity, hatred, hostility, or disharmony

b. creates unrest or disorder

c. deteriorates law-and-order situation

criminalization of these online speech is unlikely to meet the criteria under the Constitution or the ICCPR for the following reasons.

(A) While protecting national symbols and history may be a legitimate aim, section 21 is overly broad and vague, and criminalizes dissent and legitimate criticism, thus failing to meet the necessity and reasonableness tests, or the qualified grounds of restrictions.

(B) Ambiguous provision, coupled with undefined terms, makes section 24 susceptible to overreach and abuse.

(C) Criminalization under section 25(1)(a) on subjective grounds—such as "offensive" or "insulting"—introduces considerable vagueness into the law and can have a chilling effect on free expression. Different individuals and groups in a diverse society hold varied thresholds for what constitutes offensive or insulting, making the provision susceptible to arbitrary, selective, and disproportionate enforcement against activists, critics, journalists, opposition members, and marginalized and vulnerable voices. This provision therefore undermines their ability to voice concerns about governance, social justice, and corruption, effectively silencing dissent and cultivating a culture of self-censorship. This poses a serious risk to democratic discourse, as individuals or organizations critical of the state may be disproportionately targeted, leading to self-censorship and reduced public accountability. Retaining section 25(1)(a) perpetuates content regulation under the guise of protecting individuals from offensive or insulting expression, extending well beyond addressing reputational harm (as in defamation) and covering any data, information, or speech that might annoy, insult, or humiliate.

(D) Criticism of the government and its actions, policies, or other national issues are criminalized under section 25(1)(b), which can lead to self-censorship and a chilling effect on public debate. Without clear and specific definitions, authorities can construe criticism of government actions or policy shortcomings as damaging to the national image, exposing individuals to criminal liability. Because open criticism and debate are essential for accountability and transparency, and such conversations enable society to address its challenges constructively, silencing criticism in the name of "preserving the national image" that prioritizes perceived state reputation over genuine public discourse is not aligned with constitutional principles and democratic values.

(E) Ambiguities around "without lawful authority" in section 26 introduces uncertainties, while absence of exemptions for journalistic activities, whistleblowing, or legitimate research risks criminalization of conduct that is in the public interest, thereby failing proportionality and necessity requirements. Furthermore, the imminent enactment of regulation on personal data protection makes this provision superfluous.

(F) While safeguarding individuals from hate speech and incitement to violence is crucial, subjective terms—such as "values" and "sentiments"—introduces vagueness and makes the provision susceptible to arbitrary and selective enforcement, especially against religious minorities, atheists, or critics of religious practices.

(G) Online defamation laws are aimed at protecting individual reputation on the internet, but its criminalization under section 29 is likely incompatible with free speech principles due to its deterrent effect on individuals from engaging in legitimate public discourses and debates, particularly on matters of public interest. It is an outdated and disproportionate tool that fails to achieve its intended goals, instead often leading to self-censorship and social inequalities, stifling innovation, journalism, and entrepreneurship, and undermining the rule of law and democracy. Civil remedies such as fines or damages, rather than criminal penalties, are more appropriate and effective, and more aligned with the principles of justice and proportionality.

(H) While hate speech or anti-incitement laws are important to address real and immediate threats to public order, current framing criminalizes mere expression of controversial or unpopular opinions, and has been abused to target minority groups or political dissidents under the guise of maintaining communal harmony. Criminalizing speech to control unrest or disorder is also susceptible to arbitrariness and abuse, as they are inherently vague and open to broad interpretation and are often used to rationalize crackdowns on political protests, activist movements, and public dissent, in contravention of the proportionality and necessity requirements.

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

ASSESSMENT

Authority conferred to DG-NCSA or LEA to "request" BTRC to remove or block content from digital platforms is ill-conceived for the following reasons.

(i) The term "request" is inherently ambiguous and contradictory in this context, creating confusion about whether it implies a mere recommendation or carries the weight of enforcement power, compounded by mandate that BTRC "shall instantly remove or block" the content with intimation to the government. If BTRC is obligated to act on these requests without the discretion to assess their validity, it

undermines the regulatory body's autonomy and turns it into a conduit for enforcing government directives, rather than an independent arbiter of digital content regulation—effectively transforming BTRC into a rubber stamping agency.

(ii) Another critical issue is whether BTRC possesses the necessary technical capabilities to effectively remove or block content, considering it has previously admitted its limitations. A technological constraint not only impedes the enforcement of the law but also risks inconsistent or delayed content removal. Contrarily, this provision, independently or read with the *Bangladesh Telecommunication Regulation Act, 2001*, creates opportunities for the regulator to enforce internet shutdowns, website censorship, and content filtering, especially when done without clear procedural safeguards, judicial oversight, or transparent review processes, contravening free speech and due process principles.

(iii) A requirement to inform the government creates a substantial risk of politicization, leading to arbitrary and potentially unconstitutional actions. It opens the door for the use of content regulation as a tool for political repression, where decisions are made not based on law, but on political expediency, potentially silencing critics, marginalizing minority voices, and creating a climate of fear for self-censorship.

(iv) Vaguely worded grounds for content removal—such as "threat to digital security," "hampering solidarity," and "inciting racial hostility"—appears to be deliberately crafted to enable authorities to exercise their power selectively and disproportionately against political dissent rather than addressing genuine content concerns, such as CSAM or terrorist content.

(v) Delegation of authority to prescribe rules without clear legislative guidelines can lead to overreach, create legal uncertainty and enforcement inconsistencies, and expand the scope of the original law beyond what was initially intended by the legislature, especially if developed without sufficient transparency or public input.

Sections 21-26, 28-29, 31—Criminal penalties for up to five years' imprisonment and BDT 10,000,000 fine

ASSESSMENT

A penalty regime imposing up to five years' imprisonment and BDT 10,000,000 fines for a broad range of offenses 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. Without 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. Added to that, the vagueness and subjectivity of these offenses, coupled with their non-bailable and cognizable nature, further exacerbate the potential for abuse. When compared to other legal provisions addressing more tangible harms—such as physical violence, CSAM, or serious financial crimes—the severity of these penalties is particularly striking.

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, spams

(D) *section 20*—modification of computer source code

(E) *section 27*—cyber terrorism

(F) *section 30*—conducting e-transaction without legal authority

(G) *section 32*—hacking

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 to critical information infrastructure, computer systems and networks, and digital devices, or attempts or abetments—fails to outline specific parameters and clear criteria for what constitutes "illegal access" (although defined in section 2) or 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 the vagueness can lead to overly broad interpretations and the provision could be used to target individuals or organizations inappropriately. 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, undermining broader cybersecurity goals.

Ambiguities undermine the principle of legality, which mandates that laws must be sufficiently clear to allow individuals to understand what behavior is prohibited, as well as freedom from arbitrary detention and right to due process. Moreover, the lack of specificity could hinder effective security measures, as effective cybersecurity legislation relies on clarity and nuances in addressing the varied levels of associated risk and impact.

(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 "collecting any data" from a computer system is treated with the same gravity as "intentionally inserting a virus or malware," despite the vastly different potential harms these actions can cause.

Additionally, inclusion of spam and marketing emails in the same spectrum as more serious cyber offenses dilutes the focus of the provision. 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) Criminalization of source code management—a routine part of software development, maintenance,

and security practices—without distinguishing between malicious actions to cause harm and those undertaken as part of normal business operations, such as debugging, vulnerabilities patches, or updating software, risks prosecution of individuals or organizations engaging in lawful activities.

Additionally, reliance on subjective terms like "hides," "damages," and "modifies" introduces interpretative challenges, which could lead to inconsistent enforcement and arbitrary application of the law. Overall, the provision is counterproductive and could stifle innovation and discourage investment, with the net effect of detrimental effects on the technology sector and hindering growth of the country's digital economy.

(E) Expressions used to define cyberterrorism in section 27 are alarmingly broad and vague, opening the door to a wide range of interpretations. For instance, terms like "jeopardize the integrity, security, and sovereignty of the state," "create a sense of fear or panic," and "adverse effect on any critical information infrastructure" are not clearly defined, leaving them open to subjective interpretation and criminalization of activities that may not constitute genuine threats to national security. Attempts to cover a wide array of activities, from unauthorized access to computers to the creation of malware, not only fails to fit the conventional understanding of terrorism but also conflates distinct types of cyber activities that require different legal and policy responses. Coupled with the severity of the penalties without distinguishing between different levels of intent and harm, the provision poses risks to fundamental rights, particularly the rights to free speech, due process, equality before the law, and protection from arbitrary state action. Hence, the provision may have unintended and counterproductive effects, as the conflation risks diluting the focus on genuinely harmful activities that pose a real threat to national security and public safety.

(F) While it is necessary to have codes to prevent illegal online transactions, the ambiguities around what constitutes "legal authority" or "illegal" in section 30 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, poor digital literacy, and lack of robust cyber infrastructure.

(G) Definitionally, the term "hacking" in section 32 fails to clearly distinguish between different types of unauthorized access or the intent behind such access, criminalizing a broad spectrum of activities. An imprisonment term of up to 14 years and criminal fine of BDT 10,000,000 are disproportionately high, particularly when compared to other offenses that may involve more tangible harm.

Sections 52—Cognizability and non-bailability of offenses

ASSESSMENT

Cognizability and non-bailability of offenses under sections 17, 19, 27, and 32 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 seemingly non-serious and vaguely defined offenses under these provisions, 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.

PRIVACY

Sections 40, 42—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—including computers, networks, and data storage devices, and to collect traffic data from individuals or organizations—as well as to arrest individuals without 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 provision, as it stands, does 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 responsibly, reasonably, proportionately, and transparently, and 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 stringent safeguards can compromise sensitive information, including personal and business data unrelated to the offense under investigation.

Sections 45, 46, 56—Disclosure and secrecy obligations, and use of information and evidence in court

ASSESSMENT

Broad investigative and enforcement powers conferred to investigating officers allow them to seize various forms of digital evidence—including computers, networks, and data storage devices, and to collect traffic data from individuals or organizations—as well as to arrest individuals without 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 provision, as it stands, does 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 responsibly, reasonably, proportionately, and transparently, and 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 stringent safeguards can compromise sensitive information, including personal and business data unrelated to the offense under investigation.

MISCELLANEOUS

Section 35—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 35 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.

Section 54—Regional and international cooperation

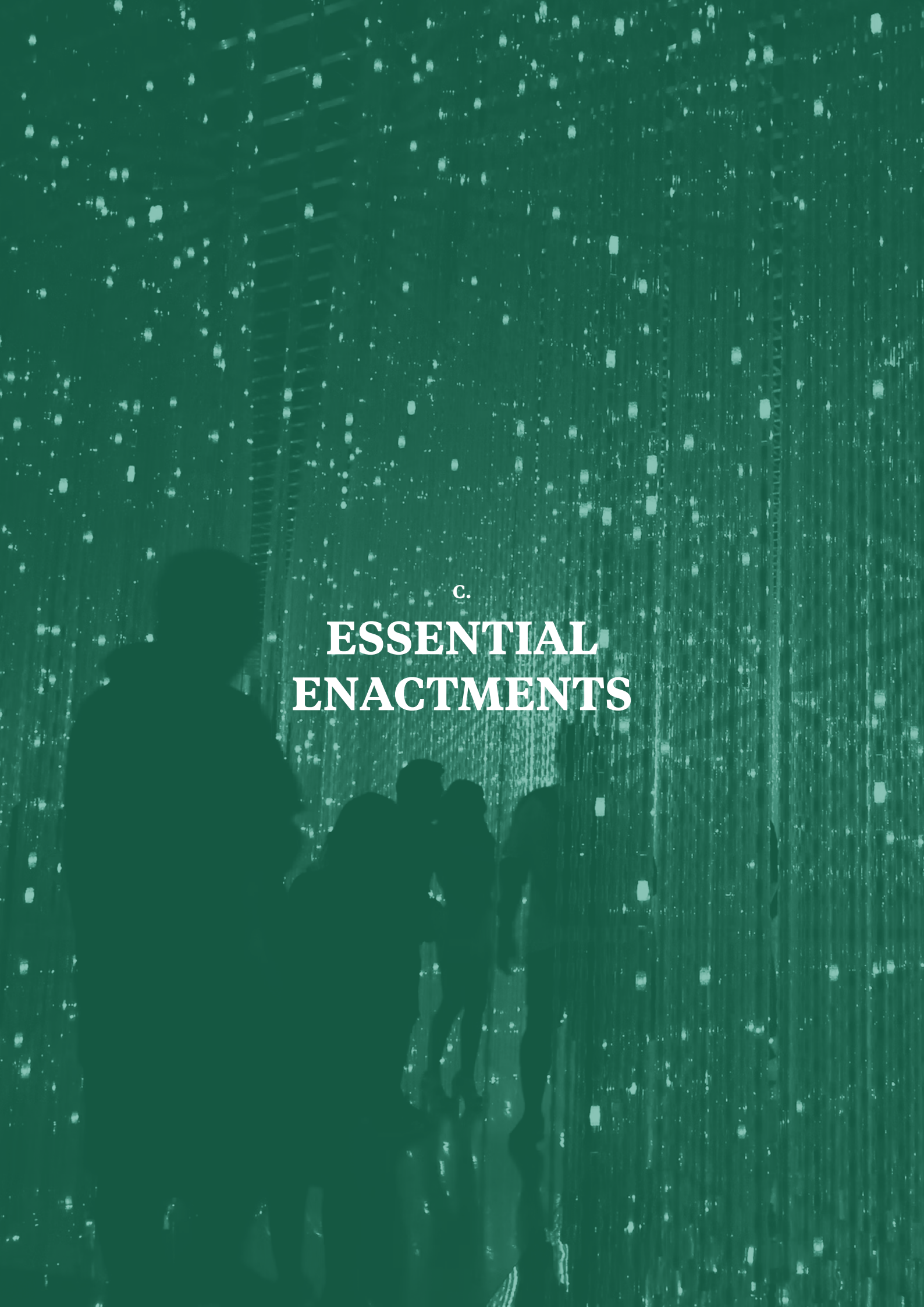
ASSESSMENT

Despite its enactment over a decade ago, the *Mutual Assistance in Criminal Matters Act, 2012*—which applies to international cooperation in the investigation and prosecution of offenses—has not been effectively operationalized, and there is a notable absence of functioning mutual assistance agreements with international counterparts. As a result of this disjunction, there are concerns about extraterritorial overreach in enforcement in transnational crimes, given the practice of BTRC of issuing orders directly to foreign companies circumventing established legal channels.

Section 59—Repealing *Digital Security Act, 2018*

ASSESSMENT

While explicitly repealing the *Digital Security Act, 2018* and allowing cases initiated under it to proceed, the provision is notably silent on the status of the *Information and Communication Technology Act, 2006*, certain provisions of which were previously repealed. This oversight raises critical questions about the continued applicability of the previously repealed provisions and the handling of cases governed by it. Absent clear guidance, this uncertainty undermines the rule of law, as it leaves unresolved issues about the legal framework applicable to cases predating the *Cyber Security Act, 2023*.



C.

ESSENTIAL ENACTMENTS

1. Online Safety Act

Objective and Rationale for Enactment

Existing laws—such as the *Cyber Security Act, 2023*, the *Pornography Control Act, 2012*, the *Penal Code, 1860*, and the *Information and Communication Technology Act, 2006*—are ill-equipped to effectively address harmful online content and cybercrimes. Equally, the proposed *Bangladesh Telecommunication Regulatory Commission Regulation for Digital, Social Media, and Over-the-Top Platforms*, mirrors the shortcomings of current legislations and is unlikely to deliver the intended outcome. Our recommendation centers on a unified legislation that addresses both content and non-content related offenses.

A statutory enactment on online content should address the increasing challenges posed by harmful online content and enhance user safety in the digital ecosystem. The proposed statute will strengthen legal mechanisms to combat online harms, setting clear and objective standards and obligations on users and digital platforms—such as social media and online communication channels—while balancing competing interests between protecting freedom of expression and ensuring public safety and order and individual dignity, as mandated by the Constitution. By establishing clear thresholds for what constitutes harmful content, it will ensure that restrictions are reasonable, necessary, proportionate, and compliant with constitutional principles and international frameworks, while mitigating risks of censorship and overreach. Particularly, the enactment should provide a framework to protect vulnerable groups, including children, women, and marginalised communities, from abuse, harassment, exploitation, and other harmful impacts of online content. Given the global nature of online harms and the reliance of digital platforms' techno-commercial models on operating from offshore locations, with no physical offices or registrations in Bangladesh, the law should expressly mandate extraterritorial application and enforcement mechanisms.

Specifically, the statute should:

(A) specify digital platforms and classes of content and services covered;

(B) establish the duty of care that digital platforms must exercise to reactively and proactively prevent the spread of harmful content, including mechanisms for the rapid detection and removal of illegal or harmful content;

(C) mandate transparency reports from platforms on content moderation practices, complaints received, and actions taken;

(D) provide clear procedures for reporting and addressing online harms, and the appeals mechanism;

(E) empower existing regulatory agencies to oversee compliance, enforce penalties, and issue guidance, with clearly set out extraterritorial application of the law and enforcement mechanisms;

(F) establish mechanisms for cooperation between government agencies, digital platforms, and civil society, both within the country and globally; and

(G) outline procedures for digital platforms to cooperate with LEAs in investigating and prosecuting online crimes.

Similarly, the statute should contain provisions addressing the unique challenges posed by cybercrimes like hacking, identity theft, financial fraud, unlawful surveillance, interceptions, ransomwares, unauthorized data modification and access, and other offenses related to digital infrastructures and other information communications technologies. The proposed statute should strengthen legal mechanisms to counter non-content technology-enabled crimes, provide individuals, businesses, and state agencies with an additional layer of defense against cyber threats, and enable more robust technological resilience and protection to critical infrastructures. With objective standards and clearly defined obligations on users and service providers, and authority and tools conferred to LEAs to investigate, prosecute, and deter cybercrimes, the statute will ensure protection of fundamental freedoms while safeguarding national security and individual rights. By developing a cohesive law that incorporates both preventive and punitive measures, Bangladesh can effectively combat cyber threats while ensuring an environment conducive to digital innovation and economic growth.

Comparable Laws

Content-related laws

Australia

Online Safety Act 2021

Adult Cyber Abuse Scheme

Abhorrent Violent Conduct Powers

Regulatory Guidance
Online Content Scheme

Image-Based Abuse Scheme

Cyberbullying Scheme

Basic Online Safety Expectations

European Union

Digital Services Act

Singapore

Broadcasting Act 1994

Code of Practice for Online Safety

Guidelines on Categories of Harmful Content

United Kingdom

Online Safety Act 2023

United States

American Innovation and Choice Online Bill

Kids Online Safety Bill

Cybercrimes-related laws

Australia

Security of Critical Infrastructure Act 2018

2023-2030 Australian Cyber Security Strategy

European Union

Directive on Attacks Against Information Systems

Directive on Combating Fraud and Counterfeiting of Non-cash Means of Payment

Singapore

Computer Misuse Act 1993

United Kingdom

Product Security and Telecommunications Infrastructure Act 2022

Computer Misuse Act 1990

The Network and Information Systems Regulations 2018

Government Cyber Security Strategy

United Nations

The Convention on Cybercrime and its Protocols I and II, and the Guidance Notes

Draft of the *Convention against Crimes Committed through the Use of an Information and Communications Technology System*

United States

Computer Fraud and Abuse Act of 1986

Electronic Communications Privacy Act of 1986

2. Regulation of Investigatory Powers Act

Objective and Rationale for Enactment

The existing legal framework on surveillance, interception and intelligence gathering is a patchwork of multiple legislations and executive instruments that grants excessive discretion without sufficient procedural safeguards. Currently, 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.

Authority to undertake these activities stems from three primary sources. First, LEAs derive extensive investigative powers from colonial-era statutes like the *Code of Criminal Procedure, 1898*, which have been supplemented by more recent statutory enactments that cross-reference this code, affirming the powers of the authorities. Second, in addition to the powers conferred by the criminal code, special laws—such as the *Bangladesh Telecommunication Regulation Act, 2001*, the *Anti-Terrorism Act, 2009*, and the *Money Laundering Prevention Act, 2012*, amongst others—specifically enable authorities to compel service providers to facilitate information and intelligence gathering and disclosure. Alongside licenses issued to telecommunication operators, these laws create a framework that mandates cooperation with state surveillance efforts. Third, some agencies, such as DGFI and NSI, operate without publicly accessible mandates, relying instead on inter-ministerial orders or internal documents that lack transparency and accountability.

While the constitutional provision allows reasonable restrictions to be imposed by law on undefined national security and public order grounds, the absence of procedural safeguards and conferral of wide discretion to the agencies to enforce interception and surveillance activities can, if unchecked, lead to subjective interpretations and arbitrary enforcement by state and security agencies, besides other concerns regarding their compliance with constitutional requirements. For instance, sections 97 and 97A of the *Bangladesh Telecommunication Regulation Act, 2001* confer open-ended authority to LEAs over telecommunication systems, including the powers to carry out surveillance and interception without procedural guardrails or judicial oversight. As the laws currently in place do not adequately address the principles of legal certainty, necessity, and

proportionality, which are fundamental to protecting citizens' rights, the broad discretion afforded to state agencies risks undermining fundamental rights, such as privacy, freedom of expression, and due process. 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.

Comparable Laws

Australia

Telecommunications (Interception and Access) Act 1979

Surveillance Devices Act 2004

Australian Security Intelligence Organisation Act 1979

Telecommunications Act 1997

Crimes Act 1914

Japan

Act on Communications Interception for Criminal Investigation

United Kingdom

Investigatory Powers Act 2016

Regulation of Investigatory Powers Act 2000

Data Retention and Investigatory Powers Act 2014

Protection of Freedoms Act 2012

Telecommunications Act 1984

Code of Practice on Covert Surveillance and Property Interference

3. Personal Data Protection Act

Objective and Rationale for Enactment

A separate legislation on data protection should provide a clear and enforceable framework for data collection, including the types of information that can be collected, processed, and transferred, rules on data minimization, retention, and consent, as well as inclusion of graded civil liability provisions. Drawing on the *General Data Protection Regulation* and other global privacy laws, the rights of individuals and the obligations of data controllers and processors should be clearly outlined, with well-crafted extraterritorial provisions without overreaching into jurisdictions where it may create conflicts of law, and unambiguous definitions of key terms. The statute should include strong safeguards against unlawful surveillance, interception, and data gathering, ensuring that any state access to personal data is strictly regulated, necessary, and proportionate.

Exceptions and exemptions, such as for national security or law enforcement purposes, should be narrowly scoped, clear, and subject to strict oversight to prevent abuse. This includes judicial oversight and transparency requirements. One critical aspect is the rejection of data localization requirements, which can create unnecessary barriers to international trade and the global flow of information, and adopt alternate mechanisms, such adequacy assessments. This approach promotes global cooperation while safeguarding individual privacy.

Comparable Laws

European Union

General Data Protection Regulation

United Kingdom

Data Protection Act 2018

Singapore

Personal Data Protection Act 2012

United States

California Consumer Privacy Act of 2018

4. Digital Commerce Act

Objective and Rationale for Enactment

Current legal frameworks on e-commerce in Bangladesh—heavily reliant on soft laws such as policies, guidelines, and voluntary codes of conduct—are one-dimensional, inadequate, and ineffective. While these instruments offer flexibility and adaptability to the rapidly evolving digital ecosystem, they suffer from significant shortcomings that hinder their effectiveness; in addition to lacking binding legal authority, the inherent vagueness renders the framework ineffective, resulting in businesses exploiting ambiguities to evade compliance, leaving consumers vulnerable to unfair terms, substandard product and services quality, and inadequate remedies when disputes arise.

One of the critical flaws of soft laws in Bangladesh is the lack of clear definitions, and this enables certain platforms like Facebook or Instagram, which facilitate sales without acting as formal e-commerce platforms (since transactions may occur outside the platform), fall under the current e-commerce framework. As a result, not only these gray zones undermine the entire framework's consistency and enforceability and contribute to an unfair competitive landscape, they, coupled with a complex customs regime, creates significant barriers to cross-border transactions.

Digital commerce services cater to different target audiences and encompass various models, each with different technical and operational architectures and needs, with variations in user interfaces, security standards, payment gateways, supply chain logistics, and regulatory compliance. For instance:

(A) in business-to-consumer models, platforms (like Amazon) sell products or services directly to individual consumers, with product catalogs, in-built payment gateways, inventory management systems, and last-mile delivery service, and a generally high volume of transactions with shorter sales cycles compared to business-to-business models.

(B) in business-to-business models, platforms (like Alibaba) are predominantly involved in transactions between businesses, such as manufacturers selling to wholesalers or retailers, with more complex operational and logistical systems involving bulk ordering, customized pricing, and integration with enterprise resource planning systems, and generally reliant on long-term relationships, larger order values, and sometimes extended payment cycles.

(C) in consumer-to-consumer models, platforms (like eBay, Craigslist, Facebook Marketplace, and TikTok Shop) integrate e-commerce functionalities to facilitate consumers selling to other consumers, often relying social influence, user engagement, and targeted advertising to drive sales, but secured by on platformed escrow payment services or in-built payment gateways, user verification protocols, and dispute resolution mechanisms, with the platforms itself having limited control over product quality and fulfillment logistics, relying on peer-to-peer communication and trust between individual users.

(D) in consumer-to-business models, individuals offer products or services to businesses (such as Upwork and Shutterstock), enabling individual users to submit proposals or bids for work, while the platform focuses on connecting businesses with freelancers and service providers, contract and project management, and secure payment solutions for freelance services.

(E) in business-to-business-to-consumer models, companies sell products or services to other businesses, who then sell them to consumers (such as third-party sellers selling to consumers via Shopify or Amazon), with the system architecture reliant on platform integration that facilitates the management of both wholesale and retail relationships, multi-tier pricing models, seamless inventory and logistics management, secure payment solutions, product customisation, and omnichannel fulfillment.

(F) in mobile commerce models, services are offered, and transactions are completed, through mobile devices, such as smartphones and tablets (such as Uber, bKash, or Apple Pay), which are reliant on native mobile applications, or mobile-optimized websites, with secure payment gateways and multi-service integrations.

Other forms of e-commerce services also operate in Bangladesh using specialized or bespoke commercial models, such as business-to-government models where companies provide products or services to government agencies using dedicated procurement platforms, and government-to-consumer models where state apparatuses offer services directly to citizens through online platforms, such as payment disbursements during COVID-19 crisis via mobile financial services—and these require special consideration depending on nature, objective, and legal system governing the services.

Even within each sub-category, there are differences in techno-commercial models. For instance, while both Facebook Marketplace and TikTok Shop has consumer-to-consumer models, the former offers a platform for users to advertise products and services which then leads to offline transaction (via mobile financial services or bank transfers, or cash on delivery), while the latter has integrated payment gateways that enable transaction to be concluded on-platform—and these technical and operational differences necessitate careful calibration the law to both meet the requirements of different services. A one-size-fits-all solution would result in ineffective and unenforceable regulatory framework.

Constitutionally, such a law would secure the rights of consumers and businesses by providing legal certainty and protecting against unlawful practices in the digital space, as well as upholding constitutional guarantees of rights to freedom of contract and property, and to engage in trade and business without unreasonable restrictions.

As such, there is an urgent need to:

(A) enact a comprehensive digital commerce statute in Bangladesh that provides clarity to businesses and consumers alike, with well-constructed and clear definitions to accommodate different techno-commercial models;

(B) establish clear, narrowly scoped extraterritorial provisions to avoid overreach while ensuring fair treatment of service providers operating from within and outside Bangladesh, given the global nature of e-commerce business;

(C) harmonize with and cross-reference other legal frameworks—such as those on customs, cross-border payment, consumer protection, contract, competition, data protection, cybersecurity, and intellectual property, by revising and revamping the *Customs Act, 1969*, *Foreign Exchange Regulation Act, 1947*, *Consumer Rights Protection Act, 2009, Contract Act, 1872, Competition Act, 2012, Cyber Security Act, 2023, Copyright Act, 2023, and Trademarks Act, 2009*—to ensure robust enforcement and facilitate smoother cross-border transactions for importers, exporters, and local and foreign consumers;

(D) streamline import-export and customs regulations and practices, and address corruption in the ecosystem, to accommodate the fast-paced nature of e-commerce, while simplifying procedures for both high- and low-value shipments and enhancing the operational capacity of state apparatuses;

(E) establish a legal basis for e-commerce contracts, ensuring they are enforceable and binding, with particular attention to the terms and conditions provided on websites, outlining how consumers can use services, return and refund policies, statutory guarantees, intellectual property protection, limits on liability for service providers, rights and obligations of both parties, and the penalties for misuse and contraventions;

(F) incorporate guardrails to address the increasing risks faced by consumers in e-commerce, including fraud, dark patterns, misrepresentation, misleading advertisements and claims, and lack of accountability, as well as emerging harms from generative AI to promote certain products, review bombs, and innovative scamming tactics; and

(G) establish graded civil and criminal liability mechanisms, providing consumers with options for redress depending on the severity of the harm, which would incentivise compliance from businesses while offering protections that are accessible and affordable for consumers.

Comparable Laws

European Union

Digital Markets Act

Digital Services Act

Organisation for Economic Co-operation and Development

Recommendation of the Council on Consumer Protection in E-commerce

United Nations

United Nations Convention on the Use of Electronic Communications in International Contracts

UNCITRAL Model Law on Electronic Commerce

United Kingdom

Digital Markets, Competition and Consumers Act 2024
Electronic Commerce (EC Directive) Regulations 2002

Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013

Consumer Protection from Unfair Trading Regulations 2008

United States

Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Bill

The Electronic Signatures in Global and National Commerce Act

Strategic Plan 2022 - 2026 on Innovation, Equity, and Resilience: Strengthening American Competitiveness in the 21st Century

5. Artificial Intelligence Strategy

Objective and Rationale for Enactment

The rapid design, development, and deployment of AI across various sectors necessitate the establishment of a comprehensive strategy framework that addresses the legal, constitutional, social, policy, and business implications of its multifaceted application—ranging from its use in the judiciary to healthcare, education, defense, and other sectors. For example, in the judicial contexts, AI tools used for automated decision-making in sentencing and assessing risks of recidivisms warrants adherence to the principles of due process, fairness, and transparency, while there is a strong focus on privacy, consent, and accuracy in diagnostics in healthcare sector and on the values of equity and non-discrimination in education sector. Meanwhile, the increased proliferation of deep-fakes and cheap-fakes is correlated to information integrity and freedom of expression, whereas predicting security threats and surveillance capabilities requires consideration of national security threats to constitutional protections against unwarranted intrusion into citizens' privacy.

At this stage, instead of rushing into legislation, the development of a national framework and sectoral regulation is preferable and practical, as legislation tends to be rigid, difficult to adapt, and subject to political pressures that may render it obsolete as the technology evolves, ensuring that Bangladesh remains competitive on the global stage without isolating itself through overly specific or restrictive domestic laws. A national framework also fosters an environment of co-regulation, where private industry plays a role in self-regulation under the oversight of government authorities, enabling the state agencies to also develop expertise and experiment with different regulatory approaches iteratively as technology and societal concerns evolve.

While there is a need for a comprehensive national framework (such as guidelines, action plans, policy statement, framework agreements, memoranda of understanding, multi-actor agreements, codes of conduct and ethics, white papers, green papers, declarations, and so on) that addresses cross-cutting issues of ethical use, accountability, non-discrimination, and societal impact, an effective regulatory regime must be context-specific, warranting, in addition to the national framework, sectoral regulations tailored to each domain of application. Furthermore, both national framework and sectoral regulations must carefully navigate competing factors—of innovation, accountability, regulation, and non-discrimination; of encouraging lawful exploration and exploitation of AI in commercial contexts; and of mitigating risks of unintended consequences, such

as perpetuating individual and systemic bias, exacerbating social inequalities, and creating harmful or irresponsible behaviors.

Of note, AI should not be regulated as a monolithic entity, similar to how the internet and other technological tools (like a knife) is not itself the direct subject of regulation. Drawing from the "Law of the Horse" analogy—suggesting that regulation of all things horse-related under one umbrella risks unifying and conflating legal principles, as different regulations are necessary for horse sales, licensing, racing, and veterinary care—a one-size-fits-all regulatory model will not address the specific causes and effects. Similarly, a national framework and sectoral regulations should focus on specific causes and effects of AI, its impact, and its interactions with existing legal frameworks. Contextual considerations and targeted application are crucial for an effective regulatory framework.

While sectoral regulation necessitates highly nuanced and technically sophisticated craftsmanship, with a carefully calibrated enforcement regime, a national AI framework must first outline foundational principles that guide all AI systems and services, including requirements that they must be:

(A) rooted in value-centered guidelines, including accuracy, accessibility, accountability, contestability, explainability, fairness, inclusivity, reliability, robustness, safety, security, and transparency, while ensuring conformity with fundamental rights and democratic values, thus establishing a legal and ethical baseline for the development and deployment of AI;

(B) grounded in human-centered and rights-respecting values, principle, and standards, positioning humans as the central stakeholders—individuals with inherent dignity, rather than consumers to sell products to or commodities from which to extract value—and, hence, all AI systems should be designed and deployed to enhance human well-being, preserve individual autonomy, safeguard human rights, protect societal welfare, and promote environmental sustainability, thus underscoring the ethical imperative that AI serves human and societal interests, not commercial or authoritarian ends;

(C) balanced between innovation and economic growth, and safeguarding consumer protection, privacy, and human rights, with collaboration between lawmakers, technology experts, policy professionals, ethicists, marginalized communities, and civil society, ensuring that AI's development aligns with broader societal values; and

(D) aligned with international standards and best practices, facilitating participation in global governance efforts to regulate AI ethically and effectively, coherently and collaboratively, avoiding regulatory fragmentation.

Comparable Laws

Organisation for Economic Co-operation and Development

Recommendation of the Council on Artificial Intelligence

G7 Hiroshima Process on Generative Artificial Intelligence

Singapore

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

United Kingdom

National AI Strategy

United Nations

Interim Report on Governing AI for Humanity

United Nations System White Paper on AI Governance

United Nations Educational, Scientific and Cultural Organization

Recommendation on the Ethics of Artificial Intelligence

United States

National Artificial Intelligence Initiative Act of 2020

Algorithmic Accountability Bill

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

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

Executive Order on Maintaining American Leadership in Artificial Intelligence

TECHGLOBAL INSTITUTE

techglobalinstitute.com