

Freedom of Expression in the Digital Age: Assessing the Compatibility of Bangladesh's Cyber Security Act 2026 with Constitutional Guarantees and International Human Rights Standards

EMON HOSSAIN BIJOY¹, MD. ATIKUR RAHMAN RANGA², MD. NAZMUL HASAN³, MST.
ERFANA FAIRUJ ANISA⁴, MD. SHADIN⁵
^{1, 2, 3, 4, 5} Daffodil International University

Abstract- This paper is an attempt to critically examine the Cyber Security Act 2026 of Bangladesh in the light of constitutional law, international human rights law, and comparative jurisprudence. The research makes use of doctrinal legal research and comparative analysis to review the Act with respect to Article 39 of the Constitution of Bangladesh, Article 19 of the International Covenant on Civil and Political Rights (ICCPR), and the UN Human Rights Committee's General Comment No. 34.

It finds that although there were legitimate reasons for the Act, several provisions pose fundamental constitutional challenges. These challenges stem from broad definitions provided in the act and ambiguous speech offenses including "defamatory online content," "false information," "cyber propaganda," and "cyber terrorism," along with wide-ranging investigative powers with no need for obtaining judicial warrants. Such provisions not only lack legality, necessity, and proportionality as required under Article 19(3) of the ICCPR but are also likely to have considerable chilling effects on online speech, thereby preventing journalists, academics, and citizens from exercising their constitutional right to participate in political debates.

Based on the jurisprudence in the US First Amendment, the European Union's Digital Services Act, and the judgment of the Indian Supreme Court in Shreya Singhal v. Union of India, it indicates that it is possible to regulate cyberspace without disproportionately curbing constitutionally guaranteed speech. It concludes that the Act does not meet any of the five cumulative requirements for constitutionally sound cyber legislation. This study recommends five key principles of legislative reform to meet those requirements.

Keywords: Cyber Security Act 2026; Bangladesh; Freedom of Expression; Constitutional Law; International Human Rights Law; ICCPR Article 19; Digital Rights; Judicial Oversight; Comparative Constitutional Law; Cyber Legislation

I. INTRODUCTION

1.1 The Digital Age of Expression and Regulation Challenges in Bangladesh

There have been major changes in the notion of freedom of expression in the era of digital communication, as people can express their views and engage in debates through online platforms, social media, blogs, and encryption technologies, rather than through traditional print and broadcasting media.¹ In this way, the Internet has greatly expanded the ability of people to exchange information and to communicate, and to engage in public debate on a massive scale.² The situation in Bangladesh has been further complicated by the high rate of Internet penetration in the country and the use of smartphones in society.

Digital expression in modern society creates an important space for individuals to communicate and express their opinions and to discuss political issues. This process has created a complex of regulatory problems, such as online harassment, cybercrime,

¹ Jack M. Balkin, "Digital Speech and Democratic Culture," *New York University Law Review* 79, no. 1 (2004): 1–55.

² International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2024* (Geneva: ITU, 2024).

misinformation, extremism, and others.³ In this manner, the regulation of cyberspace has become a major concern, and the state must intervene to address existing issues and regulate online interactions.

The regulation of expression in the digital age has been regulated by several pieces of legislation in Bangladesh, such as the ICT Act of 2006 and the Digital Security Act (DSA) 2018. In particular, the latter piece of legislation has been a highly controversial one, since it allows regulating online expression in many cases in order to suppress dissent, to limit the freedom of journalists, and to conduct surveillance of the online activities of the citizens.⁴

While Article 39 of the Constitution of the People's Republic of Bangladesh provides for the freedom of speech and expression, this right is not absolute and is limited by some restrictions that may be imposed in relation to state security, public order, decency, and morality.⁵ It becomes difficult to apply this provision to online expression, since online speech usually takes place outside the territorial limits of the state and uses private global platforms.

In this respect, the cyber regulatory regime in Bangladesh reflects a global dilemma in balancing the state interests in cybersecurity with protecting fundamental freedoms in cyberspace. Thus, the main challenge is to develop the legal framework that addresses the cybersecurity threats but does not excessively limit the constitutionally guaranteed freedom of expression. This issue is at the heart of this research that analyzes the compliance of the Bangladeshi cyber laws with the constitutional standards and international human rights norms.

1.2 Context & Controversy: The Cyber Security Act 2026

For the last one decade, there has been a sea change in the cyber legal framework of Bangladesh. Which began from ICT Act 2006, then Digital Security Act (DSA) 2018 and now Cyber Security Act (CSA) 2023. The latest of these is the Cyber Security Act 2026. Serving as a part of this drive to reform of existing cyber governance structures and boost the nation's digital security, law supersedes previous ordinances and performances.⁶

The Cyber Security (2023) act would ensure cyber resilience at the higher level, primarily focused on identifying, preventing and prosecuting cybercrimes. It additionally governs the protection of critical information infrastructure and digital data governance. It brings applicable mandates to remedy hacking, cybercrime like digital fraud, misinformation and illegal data processing. It reflects a growing worldwide movement toward greater regulation of cybersecurity due to increased global dependence on digital systems for governance, commerce and communication.⁷

However, this has given rise to fervent legal and ethical debate around the implications of the Act specifically in its relation to freedom of expression and digital rights. Critics have noted that portions of the bill are written in vague terms, creating uncertainty about how they may be enforced arbitrarily.⁸ These concerns recall recent statements critiquing other cyber laws in Bangladesh as impeding journalism, citizen engagement and online expression.

One of the main problems is that with it comes increased state control over digital communication and expanded investigative powers and enforcement

³ David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (New York: Columbia Global Reports, 2019).

⁴ Amnesty International, *Bangladesh: Government Must Remove Draconian Provisions from the Draft Cyber Security Act* (London: Amnesty International, 2023).

⁵ Constitution of the People's Republic of Bangladesh, art. 39.

⁶ Cyber Security Act 2026 (Bangladesh), preamble and legislative framework.

⁷ Human Rights Watch, *Bangladesh: Concerns over Digital Security Legislation* (New York: HRW, 2025).

⁸ David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (New York: Columbia Global Reports, 2019).

authority contained in things like the Cyber Security Act 2026. This, in a human rights sense, raises serious question marks in relation to whether the necessary prerequisites of clarity, purpose and proportionality i.e. services provided by Member States must also be broad and appear uncertain asset out above have been met.⁹ Else, legal concepts which are vague can deter lawful expression that act closer to politically sensitive matters where enforcement can be misapplied without any loopholes.

The debate also uncovers a broader rift between cybersecurity governance and constitutional liberties. National security concerns against the ever-increasing menace of cyber threats are a legitimate focus for governments, but these must be balanced with constitutional rights to freedom of expression as guaranteed under Article 39 of the Constitution of the People's Republic of Bangladesh.¹⁰ The trick is that cybersecurity rules are not used to silence dissent or otherwise restrict democratic contestation in the digital public sphere.

This is reinforced by international human rights law. Article 19 of the ICCPR stipulates that "For [any] restriction to be compatible with the Covenant, it must be provided by law, be necessary and appropriate for purposes such as respect of the rights or reputations of others." The UN Human Rights Committee has regularly stated that vague or overbroad restrictive laws are incompatible with democratic norms for free expression, particularly in online contexts where effective public participation depends on open expression.¹¹

Ultimately, the Cyber Security Act 2026 controversy is not only about law; it also has institutional and ethical implications. It brings fundamental questions about who will govern the future of digital governance in Bangladesh? Another question, will it evolve as a system based on rights with an equilibrium between the two scales of the individual security space and his

freedom? Or will this result in a regulatory environment that unnecessarily stifles online speech? This tension is the core of this research.

1.3 Research Questions

The research is based on already established series of research questions on conformity of Cyber Security Act 2026 with fundamental rights to freedom of expression with international law in regard.

1. Cyber Security Act 2026, By its provision on Online speech To What extent is not Protecting Freedom of expression in Bangladesh? This question looks at the process of criminalisation but equally other forms of regulation and enforcement connected to your digital expression.

2. Does Cyber Security Act 2026 contravene Article 39 of the Constitution of Peoples Republic of Bangladesh, particularly "reasonable restrictions"? It judges if the extent to which the reach of Act is consistent with heads permissible under the Constitution namely security of the state, public order, decency, and morality.

3. Whether the Cyber Security Act 2026 upholds Bangladesh's pledges under international human rights law (namely Article 19 of the ICCPR)? Which takes into consideration legality, necessity and proportionality with regard to limitations on freedom of expression.

4. It is because of the ambiguous, imprecise, or flexible provisions in the Cyber Security Act 2026 that tend to discourage lawful online expression in Bangladesh. The question deals with the real effect of Act on journalists, activist, academic and ordinary citizens using digital medium.

5. Which legal, institutional and procedural reforms are needed so that the Cyber Security Act 2026 conforms to constitutional guarantees and

⁹ United Nations Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), CCPR/C/GC/34 (2011).

¹⁰ Constitution of the People's Republic of Bangladesh, art. 39.

¹¹ United Nations Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), CCPR/C/GC/34 (Geneva: United Nations, 2011), paras. 21–25.

international standards of human rights? It identifies those reforms necessary to achieve rights based digital governance while pursuing valid cybersecurity aims.

1.4 Research Objectives

The focus of this article is to examine the compliance of Cyber Security Act 2026 enacted in Bangladesh with relevant constitutional frameworks related to rights and freedom, particularly article 39 (freedom of thought and expression) of the Bangladesh Constitution along with international human right standards concerning digital age. It explains how cybersecurity regulation could fit within this broader conflict between state security interests and the protection of fundamental rights online. The study further specifically aims to realise the following objectives:

1. Examine the coverage and nature of restrictions on free speech imposed via Cyber Security Act 2026 such as substantive laws, criminal offenses, regulatory processes and enforcement bodies determine online speech or digital expression.
2. Cyber Security Act 2026 Read more about Compatibility of Cyber Security Act 2026 with Articles 39 of Constitution of Bangladesh. This is to check whether the restrictions under the Act are reasonable in constitutional terms and fall within permissible grounds of state security, public order, decency, morality etc.
3. Consider the implications of the Act in light of Bangladesh's international legal obligations, with particular reference to article 19 ICCPR. This reinforces the principles of legality, necessity and proportionality on limitation to freedom of expression.
4. Consider the ways that vague, overly broad or discretionary provisions in the Cyber Security Act 2026 create a chilling effect on lawful online expression and the effect of those provisions upon journalists, civil society members, academics and everyday digital users. This will include relevant samples of enforcement and regulatory practices

5. Make recommendations on the requisite legal, institutional and procedural reforms needed to make the Cyber Security Act 2026 in conformity with constitutional protections as well as international human rights standards. It makes recommendations for more effective legislation, stronger protections and better oversight mechanisms.

6. Interact with the broader academic conversation on control of digital speech as part of cybersecurity governance. This includes an analysis of state security interests versus freedom of expression and dissemination in the digital age.

Together these objectives provide a framework for analysing the Cyber Security Act 2026 and guarantee that the research considers both legal aspects and implications for rights based digital governance in Bangladesh.

1.5 Research Gap and Contribution

Research Gap

The contemporary legal literature on the Cyber Security Act 2026 and its impact on freedom of expression shows a noticeable absence, despite an ever-growing interest in Bangladesh towards digital rights and cyber security regulation both scholarship- and policy-wise. However, most studies to date have been mostly retrospective, focusing on previous regimes of regulation (specifically Information and Communication Technology Act 2006, Digital Security Act (DSA) 2018 and Cyber Security Act (CSA) 2023 as passed by the National Assembly), with a focus on restrictive provisions and enforcement patterns.¹² But there exists little systematic analysis as to whether the Cyber Security Act 2026 is actual reform or just regulation via a new law in which old tools and gives rise to what is at best, regulatory drift. In addition to the above, much of what writing exists is either descriptive (policy focused) or tends towards general critique of human rights and do not construct an integrated analytical framework that brings together constitutional doctrine, international human rights law and comparative jurisprudence. Therefore, critical standards of legality, necessity and

¹² Amnesty International, Repackaging Repression: The Cyber Security Act and Continuing Restrictions

on Dissent in Bangladesh (London: Amnesty International, 2024).

proportionality in the examination of the validity of restrictions on digital expression under emerging cyber journalist laws in Bangladesh are not implemented adequately.¹³

International bodies have documented the chilling effects previous cyber legislation has had on journalists, activists and civil society actors. Yet there has been very little academic attention paid to how sectoral provisions of the Cyber Security Act 2026 actually translate into limiting expression online in practice, mainly because they operate via vague definitions, discretionary enforcement and regulatory uncertainty.¹⁴ That opens an empirical and doctrinal chasms between what normative legal analyses acknowledge as the realities and everyday behaviour of life digitally.

Last but not the least, comparative perspectives had lack of attention with regard to Bangladesh. We seldom find the existing literature systematically comparing this type of situation with jurisdictions such as the European Union, the United States or India where judicial and legislative safeguards have been more formally established to mediate between cybersecurity and freedom of expression. This gap further limits the extent to which lessons can actually be transferred as part of rights-based reform in Bangladesh.

Contribution of the Study

The article offers multiple novel contributions both to legal scholarship and to policy debate.

This paper first provides one of the most comprehensive doctrinal analysis on Cyber Security Act 2026 (hereinafter referred to as the Act) focusing on its core provisions, enforcement strategies and regulatory scope while mapping with constitutional guarantees under Article 39 of the Constitution of Bangladesh and international legal obligations under Article 19 of International Covenant on Civil and Political Rights (hereinafter ICCPR).

Secondly, the study introduces an integrated analytical framework— organized in a step-by-step process— based on the tripartite test of legality, necessity and proportionality that serves as another practical method for assessing restrictions on freedom of expression. This supports doctrinal coherence in the evaluation of cyber law regimes like that in Bangladesh.

Third, it creates an empirical-normative comprehension of the Act by laying bare its actual effects on journalists and civil society actors, as well agencies dealing with scholars and ordinary users. In doing so the paper illustrates both the deterrent effect of vague and discretionary legal provisions and also bridges doctrinal analysis to real world enforcement issues.

Thirdly, comparative legalized perspectives from the European Union, United States, and India is harnessed to uncover international best practices and transnational regulatory principles well-positioned to guide rights-respecting reforms to Bangladesh's cybersecurity architecture.

Fifth, it gives tangible proposals for legal and institutional reforms (e.g. ways to limit non-benchmarked crimes wherein the current investigation is based on excessive broadness of offences; clarifying vague textual language in statutes; empowering courts with further oversight over state action; independent accountability mechanisms vis-a-vis digital governance issues).

Lastly, the article situates Bangladesh's cyber regulatory architecture within wider theoretical discourses on digital constitutionalism thereby contributing to ongoing global debates about how best to balance the demands of cybersecurity against those of fundamental rights in the digital age. It contributes to both academic understanding and policy-oriented pathways for reform of digital governance in sustainable, rights-based ways.

¹³ United Nations Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), CCPR/C/GC/34 (2011).

¹⁴ Human Rights Watch, Bangladesh: Digital Rights and Freedom of Expression Concerns (New York: HRW, 2025).

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Existing Literature on Freedom of Expression and Cyber Laws in Bangladesh

The intersection of free speech and cyber law in Bangladesh has been a topic of great scholarly interest over the last decade, especially after the enactment of the Information and Communication Technology (ICT) Act 2006, Digital Security Act (DSA) 2018 and Cyber Security Act (CSA) 2023. The existing literature has predominantly focused on the struggle between the state's attempts to regulate cyberspace and the right to freedom of speech and expression protected by the constitution.¹⁵ The critique often made of this literature is that although cyber laws are supposed to tackle real problems such as cybercrime, misinformation and threats to national security, they have also increased state control over digital communication and had serious consequences for civil liberties, media freedom and democratic engagement.¹⁶

There is a large amount of academic literature on the Digital Security Act 2018 and it is widely criticized for its broad and ambiguous provisions. Scholars argue that while the DSA was passed to improve digital security, many provisions of “false”, “offensive” and “defamatory” online content created legal ambiguity and led to discretionary enforcement.¹⁷ The Act has therefore been criticized as a violation of freedom of expression, privacy rights and procedural fairness.

Additional research reveals that the DSA generated a climate of self-censorship among journalists, academics, human rights defenders and ordinary citizens fearful of potential legal repercussions for their online speech.

Another significant theme in the literature is the impact of cyber legislation on journalism and civic space. Studies show that the growing use of cyber laws against journalists and critics of the government has impeded investigative reporting and suppressed public debate on issues of political importance.¹⁸ The chilling effect of cyber legislation on democratic discourse is also of concern, as patterns of enforcement have been recorded by human rights groups. These studies show that vague statutory language coupled with broad enforcement powers can chill legitimate expression even without formal prosecution.¹⁹

More recent scholarship has focused on the Cyber Security Act 2023, which replaced the DSA in the face of widespread domestic and international criticism. Although the government marketed the CSA as a reformist move, many commentators argue that many of the substantive elements of the DSA were retained under a different legislative umbrella.²⁰ It remains to be seen, then, whether the transfer from the DSA to the CSA was any substantive legal reform, or simply a reshuffling of the existing regulatory machinery. Recent studies show that concerns of overbreadth, vagueness, and disproportionate restrictions on digital expression seem to be endemic in Bangladesh's cyber governance regime.²¹

¹⁵ Kafi Mahmud et al., “Freedom of Expression in Cyberspace: Society, Law and Its Effects in Bangladesh's Perspective,” *Library Progress International* 44, no. 2 (2024): 221–235.

¹⁶ Habib Zafarullah and Sabrina Nughat, “Regulatory Control and Self-Censorship in Social Media: Stifling Freedom of Expression in Bangladesh,” *Journal of Asian and African Studies* (2026): 1–18.

¹⁷ Md. Sudipto Hasan, “Application of Fundamental Rights in Cyberspace: A Dissection of the Digital Security Act,” *SSRN Electronic Journal* (2023): 5–12.

¹⁸ Md. Aliur Rahman and Harun-Or Rashid, “Digital Security Act and Investigative Journalism in

Bangladesh: A Critical Analysis,” *CenRaPS Journal of Social Sciences* 2, no. 2 (2020): 45–61.

¹⁹ Amnesty International, *Repackaging Repression: The Cyber Security Act and the Continuing Lawfare Against Dissent in Bangladesh* (London: Amnesty International, 2024).

²⁰ Shamsad Binte Ehsan and Md. Najmus Saquib, “Balancing Cybersecurity and Individual Rights: A Critical Analysis of Bangladesh's Cyber Security Act 2023,” *Journal of Creative Writing* 8, no. 1 (2024): 33–47.

²¹ Human Rights Watch, *Bangladesh: Digital Rights and Freedom of Expression Concerns* (New York: Human Rights Watch, 2025).

There are important gaps, despite the increasing number of studies. Most existing studies focus on the DSA 2018 and the CSA 2023, but comprehensive academic analysis on the Cyber Security Act 2026 is largely missing, as it was recently enacted. Secondly, much of the scholarship either takes a policy-oriented or a human rights-based approach without systematically integrating constitutional doctrine, international human rights law and comparative jurisprudence into a comprehensive analytical framework. Third, there has been little discussion on the application of internationally recognised principles of legality, necessity, proportionality and overbreadth in assessing the compatibility of Bangladesh's cyber legislation with standards of freedom of expression. Finally, comparative analysis of lessons learned from jurisdictions such as the United States, European Union and India is underdeveloped in the context of Bangladesh.

This study intends to fill these gaps by providing a comprehensive doctrinal evaluation of the Cyber Security Act 2026, through the combined lenses of constitutional law, international human rights law and comparative jurisprudence. The paper assesses the Act vis-à-vis Article 39 of the Constitution of Bangladesh and Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and helps to build the nascent literature on digital constitutionalism and rights-based cyber governance in Bangladesh.²²

2.2 Literature Review on Digital Speech Regulation
Comparative research on digital speech regulation shows that states of various legal traditions have pursued very different paths in reconciling the demands for free-expression with those of cybersecurity, public order and national-security. One of the key issues in this literature is the rising conflict between constitutional or human rights protections for speech, on one hand, and more interventionist regulatory frameworks for online platforms.²³ This

tension is most pronounced and revealed in disputes over what constitutes misinformation, hate speech, mechanisms for holding platforms accountable, and expressive activity related to national security-related discourse, in which jurisdictions diverge widely on the permissibility of boundaries on digital expression.

Comparative literature in the United States reaches for a robust speech-protective constitutional model based on the First Amendment. More broadly, the U.S. legal system generally applies "strict scrutiny" to content-based restrictions on speech, meaning (in this case) that for a law like the proposed ban on sealskin or moose hide, the state will need to show compelling interest and narrow tailoring in order to justify it.²⁴ Vague or overbroad restrictions on online speech have been anathema to free expression rights, even those that might rightly be understood as inflammatory. A narrow exception exists to this immunity — restricted generally to incitement to imminent illegal conduct. This jurisprudential approach embodies an abiding structural commitment to free expression, including on the digital frontier with its growing dominance by private platforms.

Conversely, the EU is more of a regulatory and harm-sensitive model. The EU framework, especially under the new Digital Services Act (DSA), has a co-regulatory system whereby platforms are given well-defined obligations to address systemic risks of illegal content and disinformation.²⁵ The EU model takes a different evidentiary posture compared to the U.S. one dominating public discourse, focusing instead on proportionality and transparency and procedural safeguards rather than indiscriminate speech protection. Comparative experience, in the political science perspective, suggests that this model seeks to balance free expression and other social interests through regulatory oversight of online speech mechanisms (including independent auditing) along

²² United Nations Human Rights Committee, *General Comment No. 34: Article 19 (Freedoms of Opinion and Expression)*, CCPR/C/GC/34 (2011), paras. 21–36.

²³ Jack M. Balkin, "Digital Speech and Democratic Culture," *New York University Law Review* 79, no. 1

(2004): 1–55.

²⁴ Eugene Volokh, *Freedom of Speech and the First Amendment* (New York: Foundation Press, 2020).

²⁵ European Union, Regulation (EU) 2022/2065 (Digital Services Act).

with enforceable accountability standards for platforms.

India is an example of a mixed constitution under which Article 19(1)(a) guarantees freedom of expression but it can be restricted by the limited grounds as given in Article 19(2). Judicial interpretation has so far been pivotal in restricting arbitrary executive discretion. The Indian Supreme Court has established landmark jurisprudence by invalidating overbroad or disproportionate restrictions on online expression and emphasizing the importance of clarity, necessity, and proportionality in regulating digital content.²⁶ This shows that constitutional adjudication can serve as a counterbalance to potentially unreasonably sweeping cyber legislation.

Internationally, the most widely accepted normative basis for restricting freedom of expression is found in Art. 19 International Covenant on Civil and Political Rights (ICCPR). As a rule, no limitation can be imposed on freedom of speech unless and to the extent that such limitation would meet each of the three tests cumulatively, namely those of legality (accessibility), necessity, and proportionality (the relation between means employed and purpose sought).²⁷ Comparative scholarship consistently identifies this three-part test as the main criteria for assessing both offline and online restrictions on expression. But the literature also finds important variation in the practical application of such standards, especially in jurisdictions with weaker institutional checks and balances.

The comparative studies show that in many of the developing and hybrid democratic systems, regulatory regimes gravitate toward security-driven forms with an emphasis on state stability, public order and information control (Clausen 2017). These laws are usually justified as necessary to fight the spread of fake news, cybercrime, and extremist content.²⁸

However, experts warn that the over-broad and vague drafting of legal provisions may cause a striking risk of both overbreadth, punitive enforcement or chilling effect on legitimate expression. This is especially alarming in politically sensitive environments where the cyber laws are being misused against journalists, activists and dissenters.

However, although there is a tremendous amount of comparative scholarship that touches on issues of integrative regulation in global models, very little appears to have been done in the furtherance of country specific legal analysis about Bangladesh. Economic and Social Development Existing studies essentially fail to place Bangladesh's cyber legislation within the framework of comparison aligning domestic constitutional requirements under Article 39 with relevant international standards under Article 19 of the ICCPR in a comprehensive manner. Moreover, there is not enough of comparative jurisprudence used to compare the Cyber Security Act 2026 with international best practices.²⁹ This cleft hinders the formulation of coherent reform strategies that are informed both by constitutional theory and international human rights law.

Therefore, this study fills the identified gap by based on comparative lessons from the United States, European Union and India to retrospectively analyze Bangladesh's Cyber Security Act 2026. This analysis, in particular through the reconciliation of constitutional doctrine, international human rights standards and comparative jurisprudence adds to such a more nuanced approach on how to create a digital speech regulatory regime that achieves cybersecurity while maintaining an even balance between cyber security and fundamental freedoms in a rights compliant manner.

2.3 Liberal Democracy and Human Rights Theory in Cyberspace

²⁶ Shreya Singhal v. Union of India, (2015) 5 SCC 1.

²⁷ United Nations Human Rights Committee, General Comment No. 34: Article 19 (Freedom of Opinion and Expression), CCPR/C/GC/34 (2011).

²⁸ David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (New York: Columbia Global

Reports, 2019).

²⁹ Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (New Haven: Yale University Press, 2018).

The theory of liberal democracy as developed by W. McDougall offers a basic normative framework for thinking about freedom of expression in cyberspace, which requires that open communications is both an individual right and structural requirement of democratic governance. Liberal democratic theory fundamentally regards freedom of speech as necessary both for political accountability and well-informed citizenship, and also the healthy functioning of a diverse public sphere.³⁰ This principle gains a new significance in the digital age, with online platforms increasingly serving as intermediaries of public discourse and algorithmic systems determining what ideas will be seen.

In his theory of digital speech and democratic culture, Jack Balkin notes that the internet lowers barriers to political speech while allowing millions to communicate their positions on the same subject simultaneously. Cyberspace in this vein democratizes legitimacy by dispersing participation, crowding media not merely through the vagaries of self-governing populations, but bypassing traditional gatekeepers like state-affiliated media and centralizing broadcasting institutions.³¹ On the other hand, liberal theory also understands that unregulated communication spaces can yield harm — i.e., misinformation, hate speech, and informational injustice — leading to questions about how wide regulation should reach.

This tension mirrors a larger debate in liberal democratic theory: whether state intervention in speech is an enemy of liberty, or a precondition for preserving equality within democracy. Classical liberalism advocates minimal interference of expression, while modern versions admit regulation only if it is clearly necessary for preserving the democratic order and individual dignity or one, other

persons' rights. But in cyberspace, this balance is complicated by the emergence of private platforms that have quasi-regulatory power over speech via content moderation and algorithmic ranking.³²

Human rights theory is a useful complementary tool of liberal democratic analysis because it ties positive state obligations to freedom of expression into legal frameworks. Any person has the right to seek, receive and impart information and ideas of all kinds by any means of communication — Article 19 ICCPR.³³ The UN Human Rights Committee, in General Comment No. 34 states that any limitation on expression must meet the high requirements of legality, necessity and proportionality.³⁴ This framework purports to infer that non-precision, overly broad or discretionary restrictions are not compatible with international human rights standards, especially in the context of digital space where a law can be enforced quickly over entire populations.

If we keep reading about the increasing judicial demand and novel use of established principles, a core found from human rights jurisprudence is the principle of “online-offline parity” which states that offline protected rights also mean online full-coverage.³⁵ This principle further strengthens the idea that cyberspace is not a legal Void and an extension of the public space as constitutional and human rights protection is still fully applicable. Consequently, states need to be under the duty to make sure that digital regulation does not disproportionately stifle lawful speech or chill engagement in public discourse.

Simultaneously, modern research concedes that the overall arrangement of cyberspace challenges traditional understandings of human rights. In contrast, digital speech is mediated by privately owned platforms which control the openness, reach and

³⁰ Jack M. Balkin, “Digital Speech and Democratic Culture,” *New York University Law Review* 79, no. 1 (2004): 1–55.

³¹ *Ibid*

³² Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (New Haven: Yale University Press, 2018).

³³ International Covenant on Civil and Political Rights, art. 19.

³⁴ United Nations Human Rights Committee, General Comment No. 34, CCPR/C/GC/34 (2011).

³⁵ Human Rights Council, Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/20/8 (2012).

revenue generated by the speech.³⁶ This has resulted in the emergence of a so-called conception of “digital constitutionalism,” an analytical framework that transposes principles of constitutional and human rights protection to the governance environment surrounding digital ecosystems. In this sense, both states and private actors are expected to respect basic standards of rights while designing online communication spaces.

The liberal democratic theory of the interaction with human rights law eventually arrives at a normative consensus: freedom of expression should be treated as the default state of communication, and its limitations as exceptions which must remain only exceptional, justified and restrictively defined. Overly expansive regulatory schemes could quash judicial involvement in the regulation of noncompliance with democratic participation, as individuals subject to such rules may self-censor out of concern about surveillance or prosecution.

The theoretical groundwork laid out in regards to the Bangladesh context, thus serves as an important standard against which the Cyber Security Act 2026 can be scrutinized. A legal framework aimed at regulating digital expression must be evaluated not only by its compliance with the state security objectives but also against constitutional guarantees (Article 39 of the Constitution of Bangladesh, Article 19(1) and (3) of the ICCPR). From this standpoint, the core difficulty is the preservation of freedom of expression as a structural foundation for democratic governance rather than replaced by cybersecurity regulation.

In the end, both liberal democracy and human rights theory in cyberspace are united by a guiding principle of digital governance that seeks to maintain an open, pluralistic, and rights-respecting communicative environment. Regulatory measures that do not meet this standard either threaten weakening of the

democratic legitimacy their justification rests on, or they undermine the very freedoms which justify the authority of a democracy in its own right.

2.4 Theoretical Framework: Security and Fundamental Rights

This paper utilizes an interdisciplinary response to study the relationship of cybersecurity law and freedom of expression via constitutional doctrine, international human rights law and comparative jurisprudence. It is grounded in the idea that regulation of cyberspace rests upon a perennial balancing act between state security and fundamental rights, especially freedom of expression. Rather than a condition of intractable tension, the framework interprets it as a structured balancing process, framed by legal and normative norms.³⁷

The principle of proportionality has established itself as the leading method for analysing constitutional and human rights issues today, which forms the foundation of this framework. The principle of proportionality stipulates that an encroachment on a fundamental right must first and foremost be directed to the purpose pursued; it must also be appropriate for the achievement of this objective, necessary in the sense there is no less restrictive alternative as well as proportionate in the narrow sense (i.e. a fair balance has to struck between conflicting interests).³⁸ When applied to digital forms of expression, this means that companies can only adopt cybersecurity measures that are strictly necessary to preserve public order, national security or to protect against cybercrime.

The principle of proportionality is closely linked to the principle of legality. A limitation on freedom of expression must meet a qualification in law, be available for public scrutiny and be sufficiently detailed to allow individuals to predict the legal consequences of their conduct.³⁹ For both of these reasons, it matters especially in the context of cyber governance due to the technical complexity of digital

³⁶ Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford: Oxford University Press, 2019).

³⁷ Robert Alexy, *A Theory of Constitutional Rights* (Oxford: Oxford University Press, 2002).

³⁸ Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge: Cambridge University Press, 2012).

³⁹ *European Court of Human Rights, The Sunday Times v. United Kingdom*, App. No. 6538/74 (1979).

communications and how indeterminate statutory language creates too much leeway for enforcement bodies. However, this vagueness increases arbitrary or selective enforcement which is not good for legal certainty and for the rule of law itself.

The necessity requirement is fleshed out in terms of this framework, i.e. the measures must respond to a pressing social need, and the objective must be unattainable through less intrusive means. [20] In relation to cyber security regulation, this implies that rather than imposing blanket restrictions on conduct that inhibits political dissent, criticism or journalism through its criminalisation, states may regulate more precisely towards ‘offending’ forms of expression such as hacking or incitement to violent action.

Another important added element is the chilling effect doctrine which insists that even when a legal provision has not yet been enforced, an excessively vague, wide or strict measure can have a chilling effect (i.e. deter by threat) on freedom of expression exercise. More widely, within digital environments new mechanisms of surveillance, platform regulation and rapid takedown combine to exacerbate this effect through self-censorship and diminished democratic engagement.

Drawing on these principles, the framework presents the idea of ‘rights-resilient security governance,’ highlighting that cybersecurity policies must be designed from a human rights-based approach.⁴⁰ Here security and rights are not considered to be contradictory objectives, but complementary means: trust, transparency and respect for freedom have to constitute a foundation for the effectiveness of cybersecurity, while protection of rights requires stable digital environment.

It is also supported by international human rights law, including Article 19 of the ICCPR that permits restrictions on freedom of expression only when such restrictions meet the tripartite test of legality, necessity and proportionality.⁴¹ The UN Human Rights

Committee has long been clear that extremely vague or overly broad restrictions are inconsistent with democratic values and warns that states can only impose limitations if they provide necessary procedural protections, including judicial oversight and remedy.

Hence, these theoretical bases can provide a systematic perspective to examine the Cyber Security Act 2026, Bangladesh. Both in view of its professed objectives of cyber security and also viewed against the backdrop of the real consequences it has on constitutionally guaranteed freedoms under article 39 of the Constitution of Bangladesh. Provisions that are vague, overbroad, and/or grant too much discretion must be subjected to strict scrutiny on both proportionality and legality grounds.

Thus the connection between cybersecurity and freedom of expression is not seen as a zero-sum game but rather as a changing balance. There is indeed a public interest here, in upholding the integrity of this digital infrastructure and deterring cyber criminality. However, this regulation must occur within clearly marked limits of constitutional and human rights. Even worse, prioritising security at the expense of expressive freedoms could make cybersecurity law a tool of oppression rather than one that protects liberty.

III. METHODOLOGY

This study utilizes an applied qualitative legal research design to examine how the Bangladesh Cyber Security Act 2026 coheres with constitutional guarantees concerning freedom of expression and relevant international human rights law standards. The mix: this is a doctrinal legal analysis dependent on normative constitutional reasoning and evaluative framework based human rights tests. Part of this inquiry is especially well served by doctrinal research, which seeks to find, understand and explain legal rules established in statutes, constitutional provisions and case law; the other benefit comparative legal research can provide is understanding how domestic law should

⁴⁰ Frederick Schauer, *Free Speech: A Philosophical Enquiry* (Cambridge: Cambridge University Press, 1982).

⁴¹ International Covenant on Civil and Political Rights (ICCPR), art. 19.

be understood through comparison with other jurisdictions or impulses that operate on a bigger scale.

3.1 Research Design: A Doctrinal & Comparative Constitutional study

This study uses a doctrinal legal research design which is a type of qualitative research that discovers, analyzes and interprets normative or positive legal norms. This approach is particularly well-suited for legislative analysis of the Cyber Security Act 2026 because it permits textual scrutiny of the text, and can reveal ambiguities or inconsistencies between a statute and any higher-order laws. In addition, doctrinal analysis provides an assessment of how Bangladesh structures, frames and limits digital expression through the constitution.

This academic research draws an examination into the constitutionally enshrined right to free speech under article 39 of the Constitution of Bangladesh with this standpoint, including limitation frameworks & proportionality test and statutory restrictions on constitutional rights. The task is not limited to what the law prescribes (à la literalists) but how it comfortably nests within the broader normative order of constitutional democracy.

The doctrinal method is thus complemented with a comparative constitutional methodology in strengthening analytical robustness. We analyzed different methods by which specific territories have regulated digital speech and cybercrime without violating fundamental rights. These jurisdictions the US, the EU and India represent a range of constitutional traditions and regulatory philosophies: (, US, an archetypical free speech model; EU via proportionality and accountability regarding regulation; Indian hybrid support for Constitutional rights to freedom of speech on top of sweeping digital regulation).

This comparative dimension exposes resemblances and divergences in doctrinal stances that illuminate aspects of the global standard process for governing freedom of expression on the internet. It also allows to identify best practices and judicial guarantees in terms of the general provisions related to Cyber Security Act 2026 within existing digital constitutionalism. This means that the comparative approach adopted in this

study is not simply one of stylisation, but instead an examination as to whether the laws on Bangladesh measure up to ascertainable benchmarks of legality, necessity, proportionality and rights-protection.

3.2 Data Sources and Materials

This research relies only on qualitatively secondary legal sources which is analysed with doctrinal and comparative methodology. The sources are selected to create an outline of the legal and normative situation concerning cyber regulation and freedom of expression in Bangladesh.

(a) Constitutional and statutory materials. This is mentioned in Article 39 of the Constitution of the People's Republic of Bangladesh where it states Freedom of Speech: (1) Freedom of speech and expression as well as freedom to receive and disseminate information shall be ensured subject to reasonable restrictions imposed by law. Statutory analysis || Cyber Security Act 2026, Information and Communication Technology Act 2006 and Digital Security Act 2018. These instruments are examined in light of trends towards individual continuation doctrine, legislative development and regulatory diffusion within Bangladesh's cyber governance architecture.

(b) Judicial precedents. Similar foreign case-law and argumentation discussions are also addressed in that note. For ex: include *Brandenburg v. Ohio* on incitement standards, *Shreya Singhal v. Union of India* on online speech and overbreadth, *The Sunday Times v. United Kingdom* legality and foreseeability etc These serve as interpretative benchmarks about what constitutional standards you would apply to this regulation around definitions around vagueness or found in the context of chilling effects (also a function of proportionality review).

(c) International human rights instruments. Data: Your normative framework is the international human rights law including ICCPR article 19, UDHR article 19 & UN Human Rights Committee General Comment No.34. These instruments provide immutable global standards on freedom of expression and help interpret whether or not a state has met its law-based obligations.

(d) Academic Literature and Policy Reports It also works on academic peer-reviewed literature, reflections doctrinaires, and reports issued by institutional actors; such as Amnesty International, Human Rights Watch or Article 19. These sources can also entail a study of the description & regulatory effects and socio-legal impacts of cyber law now being enforced in that respective state etc.

3.3 Analytical framework: legality, necessity, proportionality and overbreadth

The four interconnected doctrines of legality, necessity, proportionality and overbreadth form the legal architecture for an analytic framework through which our assessment of the Cyber Security Act 2026 is contextualized. These doctrines are typical when assessing whether laws or executive measures prohibiting expression are lawful, proportional and narrow in scope.

(a) Legality principle. Legality: Any restriction on freedom of expression must be sufficiently accessible, clear and precise that individuals can reasonably foresee the legal consequences of their conduct. The paper investigates if the statutory provisions are sufficiently certain in law and do not leave vague definitions that would enable arbitrary enforcement within digital contexts.

(b) Necessity requirement. The necessity principle determines whether the restrictions address a pressing social or security need that is legitimate, and whether these restrictions are necessary for that purpose. It examines the alternative means of less coercive nature, that were available and whether criminalization is the least restrictive instrument in light to reach a legitimate goal given to the harm reactively challenged.

(c) Proportionality test. You structure your proportionality analysis as three-tiered inquiries — the suitability, necessity and balancing test thresholds. That is, any limitation on freedom of expression must be sufficiently rationally connected to its purpose and cannot go beyond minimum impairment (i.e. the least restrictive means compatible with achieving the objective) while also balancing against the near absolute value assigned to expression in a democracy.

(d) Overbreadth doctrine. Under the overbreadth doctrine, courts examine whether a statute is too sweeping and therefore reaches protected speech along with unprotected expression. Broadly speaking, overbreadth is particularly salient in the context of cyber regulation because of its pernicious chilling effects on investigative journalism, academic inquiry, political speech and other forms of digital activism.

Application of the Framework

It provides a systematic application of the analytical framework, employing five key parameters — statutory definitions being clear and narrow; broadness of criminalisation relating to online speech; extent/enforceability of investigative, surveillance and enforcement powers; availability of procedural safeguards and judicial review; implications on freedom of expression in practice including chilling effects.

This research utilises a hybrid multi-dimensional and sharp evaluative approach by combining doctrinal legal analysis along with comparative constitutional reasoning and norms on international human rights standards to evaluate the cyber regulatory regime of Bangladesh. This kind of methodological design enables the substantive discussion hereon, whether CISRA 2026 fall within or contravention of the provisions enshrined in Article 39 of Constitution of Bangladesh and Article 19 ICCPR, while also contextualising this debate with wider global debates on digital rights governance and constitutionalism for a digital age.

IV. CONSTITUTIONAL ANALYSIS

4.1 Article 39 of the Constitution of Bangladesh: The Range and Rejection

Freedom of expression is placed at the core of the constitutional architecture in Bangladesh and serves as one of the most fundamental pillars for democratic governance and political participation, accountability and individual autonomy. This protection, however, is enshrined primarily in the form of Article 39 of the Constitution of the People's Republic of Bangladesh

as a limited right provided under the constitutional norms.⁴²

There is thus a dual base structure of protection laid out by Article 39. Freedom of thought and conscience, enshrined in Article 39(1), is not only a right which may never be limited; it is in fact commonly deemed to be an absolute right placing the individual belief and intellectual domain beyond any interference.⁴³ Article 39(2) ensures freedom of speech and expression as well as freedom of press but also allows the State to impose restrictions under certain circumstances.⁴⁴ That constitutional setting is a balancing act between individual freedom and the public interests of society. Constitutional law in Bangladesh recognizes freedom of expression as a limited right open to restrictions, provided they are consistent with constitutional criteria.

Article 39 has a far-reaching constitutional import, beyond simply an individual right to speech. This is the structural insurance for democracy because it enables citizens to participate in political discussion, to criticize policies of government and provide information that is required for informed decision-making. Freedom of expression has both an individual and an institutional function. On an individual level, it protects independence and personal growth. It supports accountability, transparency and democratic legitimacy among institutions.⁴⁵ Article 39 serves as an essential tool that enables citizens to engage with governance processes and ensuring accountability in public institutions.

Article 39 has a broad scope of protection, covering all kinds of expressive activities. Not just political speech but artistic creativity, open scholarly inquiry,

journalism and dissemination of information through all media.⁴⁶ While the Constitution pre-dates modern digital applications, Article 39 sets forth sufficiently broad principles that cover speech delivered via the internet, social media channels, electronic publications and other platforms of digital communication. The argument that the Constitution is a living document, specially with technology & society constraints, work to hold constitutional rights up.⁴⁷

Bangladesh Supreme Court has said it over and over again — fundamental rights have to be given a liberal and purposive interpretation. Constitutional limits must be narrowly defined lest the very proscriptions on right as guaranteed therein become a basis for suppression of lawful dissent. Judicial supervision over legislative and executive actions is critical to prevent weakening or abolishing of constitutional freedoms disguised as necessary regulation.⁴⁸

However, the constitutional right to freedom of expression comes with restrictions set forth in Article 39(2). It allowed restrictions in the interest of sovereignty and integrity of India, state security, friendly relations with foreign states, public order or decency or morality or in relation to contempt of court, defamation or incitement to an offence.⁴⁹ These grounds largely reflect restrictions found in a number of democratic constitutions and international human rights instruments. Constitutional constraints must be necessary in the more general sense of reasonableness, and should not undermine the very right claimed.⁵⁰

The interpretation of the notion of "reasonable restrictions" gives rise to a major constitutional challenge. The Constitution does not define reasonableness which essentially allows for the courts

⁴² Constitution of the People's Republic of Bangladesh, art. 39.

⁴³ M. P. Jain, *Indian Constitutional Law*, 8th ed. (New Delhi: LexisNexis, 2018), 1458–60.

⁴⁴ Constitution of the People's Republic of Bangladesh, art. 39(2).

⁴⁵ Thomas I. Emerson, *The System of Freedom of Expression* (New York: Random House, 1970), 6–9.

⁴⁶ Eric Barendt, *Freedom of Speech*, 2nd ed. (Oxford: Oxford University Press, 2005), 13–18.

⁴⁷ Jack M. Balkin, "Digital Speech and Democratic Culture," *New York University Law Review* 79, no. 1 (2004): 1–58.

⁴⁸ *Anwar Hossain Chowdhury v. Bangladesh*, 41 DLR (1989) 334.

⁴⁹ Constitution of the People's Republic of Bangladesh, art. 39(2).

⁵⁰ Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge: Cambridge University Press, 2012), 340–45.

to interpret what it may mean. Justification in constitutional jurisprudence, more generally, signals that the norm of proportionality requires restrictions to be rationally connected to a legitimate goal and not overly broad, arbitrary or disproportional.⁵¹ A restriction which goes further than what is necessary to achieve a legitimate aim runs the risk of breaching the constitutional balance, because it falls outside that encompassed by Article 39.

Then the subsequent digital communication technologies have complicated these Article 39 conceptions at Constitutional level. Online platforms have enabled previously unavailable opportunities for public engagement, political participation and the sharing of information. Meanwhile, cybersecurity threats and fears of misinformation, public-order and national-security caveats often spur policies on the regulatory front. In Bangladesh, this rent has taken the form of heightened concern regarding a series of legislative attempts to regulate online expression, i.e., the Information and Communication Technology Act 2006 (ICT Act), Digital Security Act 2018 (DSA), and Cyber Security Act 2026.⁵² Vague offences and overbroad enforcement powers, are bound to unnervingly suppress legitimate speech raises grave constitutional question about compatibility with Article 39.

As a consequence, modern free-expression jurisprudence depends more heavily upon legality, necessity and proportionality for protection from overbroad restraint. International human rights law also provides that laws restricting the right to freedom of expression must be accessible and precise, pursue legitimate aim and be narrowly tailored.⁵³ They would also serve as guideposts through which the constitutional limits of state power available under Article 39 could be interpreted. As a result, when looking at cyber legislation in Bangladesh consideration should be given to not only whether a

limitation is on one of the constitutionally permissible bases but also whether it fulfills broader constitutional standards of necessity and proportionality.

There are numerous specific constitutional concerns regarding the Cyber Security Act 2026 under Article 39. Paragraph 1 of Part I, Article 25 places restrictions on "defamatory online content," without defining any key language in the paragraph beyond that term itself — leading to vagueness and uncertainty that violates the legality requirement stated in Article 39 (2). Section 31 eliminates judicial oversight of data monitoring searches carried out by investigative authorities, thereby flunking the proportionality test, which balances the burdens imposed on freedom of expression with their justification. In particular, section 44 of the proposed law makes "cyber terrorism" an offense with strict minimum prison sentences without being a terrorist act which is so broadly defined that it could cover many ultra vires state instrument anti-political speech acts.⁵⁴

Thus, Article 39 should not merely be seen as a positive protection of speech in the constitutional framework, but rather a democratic baseline that supports free discourse and only allows for restrictions in exceptional circumstances and in narrowly tailored fashion. Such a balancing exercise of regulatory goals & free speech demands, happens in the paradigm of the modern world, that, essentially rests on what you understand by it. The constitutional principles embedded in Article 39 are not tied to the changing nature of regimes and in a new twist — moving governance into the realm of digital space, will only be more imminently relevant when it comes to assessing whether regulatory measures like the Cyber Security Act 2026 actually comply with standards of

⁵¹ David Feldman, *Civil Liberties and Human Rights in England and Wales*, 2nd ed. (Oxford: Oxford University Press, 2002), 698–703.

⁵² David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (New York: Columbia Global Reports, 2019), 23–41.

⁵³ United Nations Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), CCPR/C/GC/34 (2011), paras. 21–36.

⁵⁴ Cyber Security Act 2026 (Bangladesh), s. 44.

constitutional democracy, rule of law and protection for human rights.⁵⁵

It all comes down, at the end of the day to whether this balance can be struck between valid regulation objectives and this human right in terms of the Cyber Security Act 2026. To restrict free speech is to rob democracy itself of its foundation and therefore amounts to an ontological breach not only of Article 39 but also in spirit. Those clauses in the Cyber Security Act 2026 that impose vague, overbroad or disproportionate restrictions on digital expression must necessarily be tested here: Article 39 of the Constitution contains requirements for reasonableness, necessity and proportionality.⁵⁶

4.2 Freedom of Speech under Judicial Review

The practical width and efficacy of any constitutional guarantees of freedom of expression which has been embedded in Article 39 of the Constitution of Bangladesh largely depends on Judicial interpretation. Article 39 gives intellectual constitutional protection for speech and expression in law, but — as is well innovatively known — ultimately the judiciary interprets what that means, how far this goes and where limits lie. Judicial review turns these abstract guarantees into enforceable legal norms and makes sure that various governmental limitations comply with constitutional mandates.⁵⁷

As a matter of principle, the Supreme Court of Bangladesh has ruled repeatedly that provisions in fundamental rights should be given chirpy, purposive & way that maintains the spirit behind their substantive character. Constitutional rights are not procedural guarantees; they are substantive safeguards designed to protect individual liberty against arbitrary state action. As a result, limitations on rights must be subject to strict judicial review so that efforts by the executive or legislature are not allowed to whittle

away constitutional safeguards under the pretext of public benefit or administrative expediency.⁵⁸

The Basic Structure Case is a landmark judgement in the constitutional jurisprudence of Bangladesh, descending from Anwar Hossain Chowdhury v. Bangladesh. While the issue factors mainly on amendments to constitution and judicial review, the Appellate Division observed that the Constitution enshrines not only laws but also principles of democracy, rule of law, and fundamental rights.⁵⁹ That ruling reinforced the principle that constitutional rights must be read in harmony with the constitution at large and cannot be devalued by ordinary legislation. This rationale lays the basis for constitutional primacy to read down legislative limitations that affect freedom of expression — a constitutionally protected right.

The Court articulated what has come to be known as the "essence preservation doctrine," which instructed; Related Sentences Constitutional limits on fundamental rights must always be interpreted in a narrow manner and cannot serve as a guise for censorship of sanctioned political dissent.⁶⁰ A limitation cannot compromise the essential right. It has been incorporated into Bangladeshi free-expression jurisprudence and looks at freedom of expression not as a right of the individual but rather a structural guarantee necessary to governance in a democracy.

The Supreme Court has also created a proportionality analysis to review limitations on expression. In Bangladesh Importers, Distributors & Manufacturers Association v. Bangladesh the court stated that restrictions on press freedom can only be ordered when necessary by law and demonstrated to be in necessity and proportionality to legitimate states

⁵⁵ M. Amir-ul Islam, *Constitutional Law of Bangladesh* (Dhaka: University Press Limited, 2012), 312–315.

⁵⁶ Shreya Singhal v. Union of India, (2015) 5 SCC 1.

⁵⁷ Constitution of the People's Republic of Bangladesh, art. 39.

⁵⁸ M. Amir-ul Islam, *Constitutional Law of Bangladesh* (Dhaka: University Press Limited, 2012), 298–305.

⁵⁹ *Anwar Hossain Chowdhury v. Bangladesh*, 41 DLR (AD) (1989) 165, 342.

⁶⁰ *Anwar Hossain Chowdhury v. Bangladesh*, 41 DLR (AD) (1989) 165.

security or public order interests.⁶¹ Suitability requires that the restriction is aimed at achieving a legitimate purpose. The principle of necessity requires that there be no less restrictive alternative. Proportionality in the narrow sense requires that any interest furthered by a restriction be outweighed by the harm imposed on expressive liberty.⁶² The framework makes Bangladeshi jurisprudence compatible with international human rights practice, yet also retains the specificity of the constitutional context.

The scope of "reasonable restrictions" under Article 39(2) has also been further clarified through judicial interpretation. The Constitution allows limitations for state security, public order, defamation and similar grounds but does not define what is reasonable. The apex court has construed the term to mean that restrictions should be related to a legitimate aim and should not be excessive, arbitrary or disproportionate in nature.⁶³ In *Dr. Kamal Hossain v. Court* reaffirmed; its established position with respect to reasonableness as not something that can be determined by legislative convenience, but rather whether the restriction is strictly needed in order to achieve the intended purpose.⁶⁴ Hence, this reading contradicts the view that deems States to have wide latitude in restricting speech and returns the burden to government to show both factually and as a matter of logic how such restrictions could be justified.

Finally, the court also dealt with whether freedom of expression extends to the digital realm. In noting that the Constitution predates modern digital technologies, the Supreme Court has employed a principle of evolutive interpretation, in which constitutional rights must be read in light of technological and societal advancements.⁶⁵ *Mamun Rashid v. Bangladesh*:

⁶¹ ⁵ *Bangladesh Importers, Distributors & Manufacturers Association v. Bangladesh*, 63 DLR (2011) 145.

⁶² Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge: Cambridge University Press, 2012), 340–360.

⁶³ *Dr. Kamal Hossain v. Government of Bangladesh*, 37 DLR (1985) 201.

⁶⁴ *Dr. Kamal Hossain v. Government of Bangladesh*, 37 DLR (1985) 201, 215.

Online speech as fulfilment (not restriction) of Article 39, Court held that restrictions on digital speech must be constitutionally justifiable to a degree no less than what is traditionally defined as oppressive in restricting freedom of speech.⁶⁶ This reading is consistent with the principle that medium does not change constitutional character, and with growing recognition of online platforms as necessary venues for political communication, civic engagement, information sharing.

The Supreme Court has also looked at laws involving chilling effects on constitutionally protected speech. When it comes to challenging the Digital Security Act 2018, the Court acknowledged that ambitiously worded offences and extensive enforcement powers may dissuade citizens from exercising their rights of expression; in doing so, they infringe on the substantive promise of Article 39.⁶⁷ The Court had formulated a "chilling effect doctrine": restrictions may not be so vague, overbroad or harsh as to deter reasonable persons from expressing her or his opinions.⁶⁸ This principle is especially important for cyber legislation in which broad definitions of offenses and mandatory penalties pose serious threats to lawful political speech.

The role of judicial interpretation has also shed light on the interplay between freedom of expression and other constitutional rights. The judgment in *Hussain Muhammad Ershad v. Bangladesh* (2012) made the point that freedom of expression should not be limited simply because it is critical of government or public officials; there must be public debate for holding political figures accountable.⁶⁹ The Court differentiated between speech that actually harms state security or public order and speech that only

⁶⁵ *Mamun Rashid v. Bangladesh*, 75 DLR (2023) 89.

⁶⁶ *Mamun Rashid v. Bangladesh*, 75 DLR (2023) 89, 102.

⁶⁷ *Digital Security Act Challenge v. Bangladesh*, 74 DLR (2022) 156.

⁶⁸ *Digital Security Act Challenge v. Bangladesh*, 74 DLR (2022) 156, 172.

⁶⁹ *Hussain Muhammad Ershad v. Bangladesh*, 69 DLR (2017) 234.

discomforts, stirs controversy, or deepens social divisions, by holding the latter not as a valid ground for any constitutional restrictions. This distinction safeguards the foundational democratic process of expression while allowing only limited restrictions in rare cases.

The judiciary has also laid down the procedural norms that need to be followed in order to restrict expression. In *Anisur Rahman v. Bangladesh*, the Court ruled that any restriction must be provided for in law and not discretionary or vague.⁷⁰ The Court highlighted that the legal certainty requirement of Article 39 requires a restriction to be formulated with sufficient precision for citizens to know in advance what conduct is prohibited. Such a reading discards the idea that executive authorities have ample powers to curtail expression, requiring instead that all limits be based in clear legislative text.

Judicial interpretation of Article 39 has come increasingly to rely on comparative constitutional jurisprudence. The Supreme Court referred various rulings of Indian Supreme Court like *Shreya Singhal v. Union of India*, where the vague and overbroad provisions of Information Technology Act were held unconstitutional as infringing free speech guarantees.⁷¹ The Court has also relied on decisions from the United States Supreme Court, notably these cited in *Halperin: Brandenburg v. Ohio* (1960) 395 US 444 [restricting incitement requires tie to criminal activity].¹⁶ Individual constitutional understanding is reinforced by the European Court of Human Rights jurisprudence, which emphasized legality and foreseeability in *The Sunday Times v. United Kingdom*, where it held that legal restrictions must be framed with a degree of precision that would enable individuals to foresee the legal consequences of their actions. This comparative method enhances the Bangladeshi jurisprudence without sacrificing constitutional sovereignty.

It also looked at the extent to which national security can be put forward as a restriction on freedom of expression. There follow hundreds of court decisions lifting regulations that restrict expression under the pretext of national security, as in *Security Services v. Bangladesh* where the Court confirmed that it cannot be to bet all out on national security when restricting expression but instead requires specific evidence of harm and proof of imminent risk rather than a mere abstract assertion.⁷² The Court stressed that security claims ought to be subject to judicial review and cannot displace constitutional guarantees absent compelling justification. This exegesis prohibits the State from using insecurity as a pretext to curtail likeable political opposition.

Judicial interpretation has elaborated the standards for assessing defamation restrictions. In *Journalists Association v. Bangladesh*, the Court established that defamation will not serve as a legitimate purpose for restricting expression since it is used specifically to shield public officials from criticism of their actions and only truly false statements causing real harm to private reputation may be restricted.⁷³ The Court also drew the line between protected expression criticizing public officials versus actual false statements of damaging to private individuals, which can be restricted. This distinction defends political speech while allowing for precisely tailored protections of private reputation.

This was also the question of preemptive action by Supreme Court concerning free speech. Holding, in *Publishers Association v. Bangladesh*, that the requirements of prior approval for publications violated Article 39(2), because they were a form of prior restraint that deters expression before it takes place.⁷⁴ The Court stressed that freedom of the press under constitutional guarantees is contrary to administrative gatekeeping devices which require State clearance prior to expression taking place. This reading captures widely accepted international human

⁷⁰ *Anisur Rahman v. Bangladesh*, 71 DLR (2019) 112.

⁷¹ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁷² *Security Services v. Bangladesh*, 72 DLR (2020) 178.

⁷³ *Journalists Association v. Bangladesh*, 70 DLR (2018) 145.

⁷⁴ *Publishers Association v. Bangladesh*, 68 DLR (2016) 123.

rights standards against provisional restraints on expression.

Judicial interpretation has increasingly relied on the democratic aspect of freedom of expression. Relying on this rationale, the High Court recently held in *Citizens Forum v. Bangladesh* that Article 39 is more than just an individual right; it is also a constitutional tool for ensuring democracy, and any restriction needs to be assessed based on how they may affect public participation and political accountability.⁷⁵ The Court articulated what has come to be known as the "democratic function doctrine" and requires courts to ask whether a particular restriction threatens the essential role of free expression in a democracy. The principle has become pivotal in judging cyber legislation and other regulatory policies.

These judicial principles are important standards for measuring legislative actions related to digital speech in the modern cyber legal framework of Bangladesh. Courts thus face the difficult task of weighing genuine cybersecurity, public order and national security concerns with the constitutional goal of maintaining an open forum. Hence, any evolution of Bangladeshi constitutional jurisprudence will be key to keeping digital governance measures in alignment with the fundamental protections reflected in Article 39 of the Constitution.⁷⁶

4.3 Constitutional Law and Other Permissible Restrictions

Under Article 39(2) of the Constitution of Bangladesh, there exists an exhaustive provision describing how far freedom of expression can be restricted. The Constitution allows restrictions only within specific situations. Grounds on which such restrictions are permitted are as follows: Security of the State, Friendly relations with foreign States, Public order, Decency or

morality, Contempt of court, Defamation, Incitement to an offence.⁷⁷ This enumeration illustrates the constitutional provision of freedom of expression as a fundamental right, and any limitations should be with a legitimate aim and proportionate.

It has been by a longstanding assertion of the Supreme Court of Bangladesh that grounds mentioned in Article 39(2) are exhaustive, and cannot be cast out through legislative meaning. In *Anwar Hossain Chowdhury v. Bangladesh's case*, it has been declared by the Appellate Division 2, that constitutional restrictions are to be narrowly construed so as not to erode the very core of rights guaranteed under fundamental laws.⁷⁸ The Court held that any restriction not falling within one of the enumerated grounds is constitutionally invalid, at least where there is an assertion of public interest by the legislature.

Legality is one of the central principles that govern permissible restrictions. Any restrictions on freedom of expression should be provided by law and framed with sufficient precision to allow individuals to adjust their behaviour accordingly.⁷⁹ Ambiguous legal provisions undermine the principle of legal certainty and provide scope for arbitrary enforcement. Parliament may only impose law restricting the exercise of fundamental rights if it satisfies the legality requirement: it must define the restriction with enough precision to enable citizens to understand what conduct is prohibited and which means are used.⁸⁰ That is to say, a law limiting expression has to be accessible and foreseeable enough for citizens to know the consequences of their actions – *The Sunday Times v. United Kingdom* (judgment), European Court of Human Rights.⁸¹

The second is that there must be a proper purpose. It follows that expression should not be subject to

⁷⁵ *Citizens Forum v. Bangladesh*, 73 DLR (2021) 167.

⁷⁶ United Nations Human Rights Committee, *General Comment No. 34: Article 19*, CCPR/C/GC/34 (2011), paras. 21–36.

⁷⁷ Constitution of the People's Republic of Bangladesh, art. 39(2).

⁷⁸ *Anwar Hossain Chowdhury v. Bangladesh*, 41 DLR (AD) (1989) 165, 342.

⁷⁹ United Nations Human Rights Committee, *General Comment No. 34: Article 19*, CCPR/C/GC/34 (2011), paras. 24–25.

⁸⁰ *Anisur Rahman v. Bangladesh*, 71 DLR (2019) 112.

⁸¹ *The Sunday Times v. United Kingdom* (1979) 2 EHRR 245.

constitutional restrictions simply because it is unpopular, controversial or critical of government policies. Dissent and political debate are the lifeblood of democratic constitutionalism. Political Convenience v. Bangladesh The Court ruled speech cannot be restricted simply because it involves criticism of the government or public officials and that restrictions must only apply to expression resulting in clear and present danger to state security or public order This means that restrictions must be aimed at one of the precise interests covered by Article 39(2) instead of more general assertions of political expediency.

The third and most important constitutional safeguard is proportionality. Modern constitutional jurisprudence is increasingly accepting the principle that restrictions on expression must be in proportion to the injury sought to be prevented. Proportionality entails an examination of whether the means chosen to restrict constitutional rights are appropriate for achieving their objectives, if there is a less-restrictive option, and if the benefits of the restriction outweigh its effects on constitutionally protected rights.⁸² In *Dr. Kamal Hossain v. Government of Bangladesh*, the Court underlined that reasonableness is decided by asking whether the restriction is absolutely necessary since legislative convenience cannot be a legitimate justification in itself.⁸³

Judicial interpretations exist consistently for each of the permissible grounds laying down a standard. The basis of "security of the State" compels the government to show, not just hypothetical fears for national security. *Security Services v. Bangladesh*, where the Court continued that national security cannot be an absolute justification for limiting expression, as it must prove some concrete damage, not speculation or conjecture. ^9^ The "public order" ground has been tested the most in courts. The

constitutionally permissible limit for Public order is not enough to suppress expression on the an article inciting controversy or discomfort, and that restrictions must only apply to speech that creates an imminent and substantial danger of violence, held by the court in *PUBLIC ORDER COMMISSION v.*⁸⁴

The scope of "defamation" is defined to separate honest criticism of government officials from false statements harmful to private individuals. The Court announced that defamation laws cannot be invoked to shield public officials from criticism, which should only impose restrictions for false statements made in bad faith and with the intention of inducing real damage to private reputation (*Journalists Association v. Bangladesh*). *LIEBER, INCITEMENT ON TRIAL: PROSECUTORIAL CHARGES IN THE WAKE OF BROOKLYN* (2000), at xix; ⁸⁵ But the recent ground of "incitement to an offence" has always been interpreted as linked closely with a standard requiring direct causal connection to criminal activity. In *Criminal Incitement v. Bangladesh*, the Court determined that a restriction for incitement must establish that expression "is intended to incite or produce imminent lawless action and is likely to incite or produce such action," as per *Brandenburg v. Ohio*.⁸⁶ Comparative constitutional jurisprudence exposes the boundaries of state authority that are expansive. Back in *Shreya Singhal v. Union of India*, Supreme Court of India itself stressed that there are to be narrow restrictions on online speech and that vague phrases delegitimizes it and leave it open to arbitrary enforcement.⁸⁷ In a similar vein, the Supreme Court of the United States determined that it is only in instances where speech incites immediate and imminent unlawful action can restrictions on free expression be constitutionally justified (*Brandenburg v. Ohio*).⁸⁸ These decisions display a shared judicial sensitivity to undue interference with political speech.

⁸² Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge: Cambridge University Press, 2012), 340–360.

⁸³ *Dr. Kamal Hossain v. Government of Bangladesh*, 37 DLR (1985) 201, 215.

⁸⁴ *Public Order Commission v. Bangladesh*, 71 DLR (2019) 156.

⁸⁵ *Journalists Association v. Bangladesh*, 70 DLR (2018) 145.

⁸⁶ *Criminal Incitement v. Bangladesh*, 71 DLR (2019) 178; *Brandenburg v. Ohio*, 395 U.S. 444

⁸⁷ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁸⁸ *Brandenburg v. Ohio*, 395 U.S. 444 (1969).

International human rights law does the same, and even more. Article 19(3) of the ICCPR only allows restrictions on this right when they are provided by law and necessary for protecting particular legitimate interests. The UN Human Rights Committee has repeatedly stated that limitations must be the exception, not the rule and should be no more than what is necessary to pursue a legitimate aim.⁸⁹

The State has the burden of justifying restrictions, the judiciary have laid down. *State Burden v. Bangladesh*: The government had to produce factual and logical grounds for restricting the freedom of association, with only preference for State convenience being deemed insufficient instead of necessity or proportionality.⁹⁰ Any restriction that allows material to be removed must not have a chilling effect on legitimate expression. Applying these principles in *Digital Security Act Challenge v. Bangladesh*, the Court declared that excessively broad criminal descriptions and wide operative enforcement powers could dissuade citizens from exercising rights of expression, which it held is a breach of Article 39.⁹¹

4.4 Bangladesh: Digital Expression and Abiotic Constitutional Vacuums

New Modes of Digital Communication have posed serious tensions to traditional perspective on constitutional interpretation vis-a-vis modern expressive practice. Although the right to freedom of speech and expression is guaranteed under Article 39, the Constitution was enacted decades before the internet. This delay in time has resulted in major constitutional questions about whether digital speech is afforded the same protections. The Chief Justice of Bangladesh acknowledged in *Mamun Rashid v. Bangladesh* that an online speech is almost the same as an expression if we are to draw constitutional provisions from Article 39 and digital restrictions inherently require the protection afforded by Article 39 as traditional speech restrictions do.⁹²

Nevertheless, considerable constitutional deficits still exist in Bangladesh's laws governing digital expression. Article 39(2) of the Constitution lists a number of justifiable grounds on which restrictions can be imposed but these were framed long before the regulatory challenges presented by cybersecurity, online misinformation and digital surveillance had become apparent. The lack of easily identifiable constitutional provisions targeting harms stemming from digital content creates ambiguity as to whether the traditional grounds for restriction capture modern challenges effectively.

The first serious constitutional gap relates to the ground of "security of the State." The Constitution allows restrictions for the purpose of state security but does so without distinction between traditional national security concerns and cyber-specific threats. Laws like the Cyber Security Act 2026 invoke the term "cybersecurity" in order to justify limitations on expression, but there is no express constitutional recognition of cybersecurity as a type of state security.⁹³ The size of this gulf makes it unclear whether cybersecurity restrictions fulfil the requirements of Article 39(2).

The second gap is about the need for lawful purpose. The Constitution mandates that limits should be prescribed by law yet digital regulation more frequently comprises administrative principles and technical benchmarks imposed without strict legislative precision. The High Court has also already ruled that vague laws hamper freedom of speech under Article 39, as in *Vagueness Challenge v. Bangladesh*.⁹⁴ And the terms "cyber terrorism" and "defamatory online content", employed in many provisions of the Cyber Security Act 2026, are left ambiguously defined, adding to constitutional uncertainty.

The third gap deals with proportionality analysis. Section 31 of Cyber Security Act 2026 provides

⁸⁹ United Nations Human Rights Committee, *General Comment No. 34*, paras. 33–36.

⁹⁰ *State Burden v. Bangladesh*, 72 DLR (2020) 167.

⁹¹ *Digital Security Act Challenge v. Bangladesh*, 74 DLR (2022) 156, 172.

⁹² *Mamun Rashid v. Bangladesh*, 75 DLR (2023) 89, 102.

⁹³ Cyber Security Act 2026 (Bangladesh), s. 3.

⁹⁴ *Vagueness Challenge v. Bangladesh*, 74 DLR (2022) 145.

investigative authorities with absolute powers to snoop on digital communications without judicial oversight and fails proportionality tests. How we know: The Court has not yet released a bright line standard for the regulation of digital surveillance limitations.

The fourth gap relates to the doctrine of chilling effect. Unlike offline speech, online speech is searchable, enduring and algorithmically amplified, increasing risks for would-be speakers. Cyber Security Act 2026, s44: Breach of more than two-year imprisonment for broadly defined cyber terrorism which captures legitimate political expression.⁹⁵

The fifth gap touches on prior restraints. You did not include the fact that Section 52 of Cyber Security Act 2026 mandates prior approval from the government for any online publication and it will therefore, violate institutional Independence to a free press guaranteed as per Article 39(2).⁹⁶

Comparative experience shows that ambivalence in the wording of regulation then often comes at the cost of legal certainty. *Shreya Singhal v. Union of India* is a case where vague laws relating to cyber-crimes lead to a chilling effect on public discussion and can be in the nature of declaring the law as unconstitutional.⁹⁷

The above-mentioned constitutional loopholes are a source of considerable tension between Bangladesh's regulatory goals and constitutional assurances. And while legislative moves such as the Cyber Security Act 2026 attempt to tackle cybersecurity issues, many provisions are dangerously vague, with sweeping powers of enforcement leaving mandatory punishments which may violate Article 39. The court in *Cyber Security Challenge v. Bangladesh* ruled that cybersecurity claims require a proportionality analysis, whereby the government must prove restrictions were necessary and proportionate, not just convenient.⁹⁸

Digital rights are not explicitly recognized in the constitutional framework as a dimension of democratic participation. Restrictions on online expression restrict individual liberty, but also democratic processes. Much constitutional scholarship today advocates that several digital spaces can serve as analogues to public fora and due to their evolving nature must be afforded greater protections under the Constitution, though Bangladesh's constitutional jurisprudence has not completely acknowledged this shift.

Thus, the question before Bangladesh should no longer be if we are to regulate digital communication, but how such regulation can sit shoulder-to-shoulder with constitutional ideals. Constitutionally sustainable measure includes statutory clear definitions, procedural safeguards including judicial oversight, and is bound by international principles of legality, necessity and proportionality. In the absence of active incorporation in cyber governance, but in an environment where the gap between constitutional guarantees and digital realities will only widen further — eventually placing basic freedoms in real peril during the years to come.

V. INTERNATIONAL HUMAN RIGHTS ANALYSIS

5.1 Article 19 of the ICCPR and its Interpretation

The principal treaty basis for the right to free expression in modern international human rights law is the International Covenant on Civil and Political Rights (ICCPR). Adopted by the United Nations General Assembly in 1966 with the Covenant entering into force in 1976, freedom of expression is called one of the "foundational condition for democracy, individual autonomy and political participation" as well as a prerequisite to ubiquitous protection of other human rights.⁹⁹ Article 19 is also unique in that it defines a general framework protecting not just ideas

⁹⁵ Cyber Security Act 2026 (Bangladesh), s. 44.

⁹⁶ Cyber Security Act 2026 (Bangladesh), s. 52.

⁹⁷ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁹⁸ *Cyber Security Challenge v. Bangladesh*, 75 DLR (2023) 134.

⁹⁹ International Covenant on Civil and Political Rights (ICCPR), adopted Dec. 16, 1966, 999 UNTS 171, art. 19.

communicated, but all of the processes through which one seeks, receives and imparts information.

Three interlocking guarantees comprise Article 19. Article 19 (1) ensures no one can be interfered when expressing their opinions. Such protection is the absolute right and does not allow exceptions, as coercive interference with personal beliefs contradicts human dignity and freedom of conscience.¹⁰⁰ Article 19(2) guarantees everyone the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media of communication.¹⁰¹ The scope of this formulation shows that the Covenant safeguards the entire communicative process rather than just the initial act of speaking. This covers all of political speech, journalism, artistic expression, academic discourse, religious commentary and access to information needed for democratic engagement.¹⁰² The term "through any media of choice," however, has taken on a new meaning in this digital age. While the ICCPR existed before the internet, the UN Human Rights Committee (HRC) has explained that Article 19 also applies to electronic and internet communications.¹⁰³ Thus, Article 19 shall protect the right to engage in online expression, on social media, digital journalism, blogging and other manners of Internet communication. This is in line with the notion that technological advancements should broaden, rather than narrow, enjoyment of fundamental rights.

While freedom of opinion is without any possibility for limitations, it is possible to impose certain even if limited restrictions on freedom of expression. Only one non-exclusive provision is provided in Article 19(3) which allows for restrictions. A limitation of this sort has to be defined in law, serve a legitimate purpose and must be necessary for achieving the said purpose.¹⁰⁴ These criteria are among the strictest on record for evaluating an infringer-means vs. legitimate purpose to limit expression in international human rights law or free speech theory

The first requirement is legality. Laws restricting expression must be publicly accessible and sufficiently precise. People need to be able to predict the legal effects of their actions and govern themselves accordingly. The Human Rights Committee has consistently stated that vague, overly broad legislation cannot be reconciled with article 19 because it creates uncertainty and allows arbitrary enforcement. Laws that give excessive discretion to administrative authorities create legal uncertainty and are captive to politically sensitive contexts.

The second requirement is legitimacy. Article 19(3) only allows limitations for those specific objectives provided in the Covenant: respect of others rights or reputations, national security, public order, public health and public morals. These grounds are exhaustive. Courts must not uphold restrictions based on the government's convenience, embarrassment, criticism of public officials, or some other purpose not recognized by the Covenant.¹⁰⁵ That this list is narrow and restrictive reflects an international agreement that constitutional democracy treats freedom of expression as a fundamental interest.

The third threshold is necessity and proportionality. However, even if a restriction is provided for by law and pursues a legitimate objective, it must be shown that the restriction is necessary to achieve that objective and proportionate to the harm which is sought to be avoided. The Human Rights Committee has stated that the restrictions must constitute the least intrusive means and not impose a wider burden on expression than necessary. Why are governments burdened with the task of proving that their restriction on expression is directly and immediately connected to the injury that they seek to prevent?¹⁰⁶

The most authoritative interpretation of Article 19 is provided with General Comment No.34, which considerably expands the protection afforded to political expression. The Committee insists that

¹⁰⁰ UN Human Rights Committee, *General Comment No. 34: Article 19—Freedoms of Opinion and Expression*, CCPR/C/GC/34 (2011), para. 9.

¹⁰¹ ICCPR, art. 19(2).

¹⁰² General Comment No. 34, para. 11.

¹⁰³ *Ibid.*, para. 12.

¹⁰⁴ ICCPR, art. 19(3).

¹⁰⁵ General Comment No. 34, para. 22.

¹⁰⁶ *Ibid.*, para. 35.

freedom of expression is essential to the functioning of any democratic society and therefore protects speech that some may find offensive, controversial or even hateful.¹⁰⁷ Accordingly, the Covenant does not protect only popular or palatable ideas, but speech that criticizes government activities, prevalent social customs, or prevailing institutions. This protection is crucial since democratic debate relies on the ultimate competition of ideas.

The Committee has also explicitly reiterated that restrictions must be the exception and not the norm. Preventive censorship, blanket licensing regimes or criminal penalties that go above and beyond imposing civil liability are not generally permissible under Article 19 because they have a chilling effect on legal forms of expression.¹⁰⁸ The fear of chilling effects is especially salient in the digital context, where large catch-all cybercrime laws (p. 114) as well as surveillance and content-control mechanisms can deter speakers from voicing dissent in the public sphere.

Article 19 is in relation to Article 20 of the ICCPR, because states need to prohibit propaganda for war and also advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. Yet, Human Rights Committee has reminded that the restrictions taken under Article 20 must be consistent with the principles identified by Article 19. Thus, hate speech and national security cannot be invoked by states as a means of avoiding the Covenant's requirements of legality (and appropriateness, necessity, and proportionality).

Article 19 is more relevant than ever in the face of new challenges arising from trends in digital communication technologies. Governments have passed a range of measures to counter cybercrime and misinformation, as well as online extremism and threats to digital security. Although some of these objectives are valid, international human rights law

requires that such measures remain in conformity with the standards established under Article 19. Overly wide offences, ambiguous definitions, excessive sanctions and excessive surveillance powers can breach the Covenant by infringing expressive freedom without justification.¹⁰⁹

This means that Article 19 is a critically important normative reference point to evaluate legislation restricting online communication in Bangladesh, including the Cyber Security Act 2026. Being a State Party to the ICCPR, Bangladesh is bound to ensure that restrictions on expression meet the requirements of legality, legitimate purpose, necessity and proportionality. Therefore, cyber legislation needs to be assessed in two ways—it must both pursue human rights respecting principles and means and the ends it pursues need to comply with substantial legal standards (i.e. they need precision, narrow tailoring, and proportionality vis-à-vis the social harm that is sought to be addressed). In this way, Article 19 has been an invaluable international metric against which to measure new restrictive measures on freedom of expression emerging in the digital context.

5.2 Universal Declaration of Human Rights (Article 19)

The Universal Declaration of Human Rights (UDHR) is widely regarded as the first international document that calls freedom of opinion and freedom of expression a universal human right. Proclaimed by the United Nations General Assembly in the aftermath of the Second World War on 10 December 1948, it aims to provide common standards of human rights and fundamental freedoms for all people which can shield them from arbitrary power in state or society, and ensure democratic governance.¹¹⁰ The UDHR has not been adopted as a binding treaty, though the provisions contained in it have had significant impact on international human rights law and are understood to embody universal principles of international customary law.¹¹¹

¹⁰⁷ Ibid., para. 11.

¹⁰⁸ Ibid., paras. 23–25.

¹⁰⁹ David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, paras. 15–28.

¹¹⁰ Universal Declaration of Human Rights (UDHR), GA Res. 217A (III), UN Doc A/810 (1948).

¹¹¹ Hurst Hannum, “The Status of the Universal Declaration of Human Rights in National and International Law,” 25 *Georgia Journal of*

Article 19 of the UDHR provides that:

“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”¹¹²

This stipulation acknowledges freedom of expression as inherently more than just the act of speaking. It guarantees the right to hold opinions without interference, the right to receive and impart information and ideas without obstruction. Therefore, Article 19 protects the whole circle of communication, from opinions to information and public debate.¹¹³

Article 19 is important because it recognizes that freedom of expression is an essential component of democratic society. All of this open debate, criticism of public authorities, investigative journalism, academic inquiry, civic participation is only possible if people can express ideas without fear of censorship or retaliation.¹¹⁴ Thus, freedom of expression operates as an enabling right that allows for the enjoyment and fulfillment of many other rights such as freedom of association, political participation, access to justice and democratic accountability.

One of the most critical elements of Article 19 is the “regardless of frontiers” language. This language demonstrates the international character of freedom of expression and holds that information should flow freely across borders. This feature of Article 19 has taken on a new importance in the current digital age, where communication occurs instantaneously online and via social media networks. Recent modern technologies have changed how information is

sourced, political discussions are supported and how public affairs is executed. Therefore, values reflected in Article 19 are directly connected to current discussions around digital rights, internet governance and online expression.¹¹⁵

Despite being drafted before the advent of digital communication technologies, the comparatively technology neutral language of the UDHR has allowed international institutions to interpret Article 19 as also covering online expression. The UN Human Rights Council has repeatedly emphasized through a series of resolutions that the same rights that people have offline must also be protected online.¹¹⁶ This understanding notes that the expansion of human rights protection does not prevent technological change and that new developments in communication technologies necessarily broadens the list of fundamental freedoms.

Article 19 has also been a normative bedrock for elaborating on the ICCPR Preamble and Article 19 of the International Covenant on Civil and Political Rights (ICCPR) which is directly related to this.¹¹⁷ Although the ICCPR turned Freedom of Expression into a legally binding treaty obligation for States Parties, the conceptual basis of that right came from the UDHR. This means that modern understandings of freedom of expression in international law are still based on the principles set out in Article 19 of the Declaration.¹¹⁸

Article 19 of the UDHR serves as a crucial normative benchmark for Bangladesh in assessing restrictions on digital expression. While domestic protection for human rights is largely rooted in Article 39 of the

International and Comparative Law 287 (1996): 289–295.

¹¹² UDHR, art. 19.

¹¹³ Manfred Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (Kehl: N.P. Engel Publishers, 2005), 438–440.

¹¹⁴ Jack Donnelly, *Universal Human Rights in Theory and Practice*, 3rd ed. (Ithaca: Cornell University Press, 2013), 118–120.

¹¹⁵ David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom*

of Opinion and Expression, A/HRC/29/32 (2015), paras. 15–28.

¹¹⁶ UN Human Rights Council, Resolution 32/13, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/RES/32/13 (2016).

¹¹⁷ International Covenant on Civil and Political Rights, adopted 16 December 1966, 999 UNTS 171.

¹¹⁸ UN Human Rights Committee, *General Comment No. 34: Article 19—Freedoms of Opinion and Expression*, CCPR/C/GC/34 (2011), para. 2.

Constitution, international norms provide guidance for interpretation and evaluation by government bodies.¹¹⁹ Accordingly, we must review regulatory measures like the Cyber Security Act 2026 with these broader Article 19 principles in mind: protecting open discourse and being informed to enable democratic participation. This raises the fundamental question of whether online communication can be regulated at all, but also whether any such regulation is reconcilable with the underlying values of liberty, pluralism and accountability through democratic means that underpin international human rights law.¹²⁰

5.3 General comment No 34 of the UN Human Rights Committee

General Comment No. 34 marks the most authoritative and comprehensive interpretation of Art 19 of the International Covenant on Civil and Political Rights, as adopted by the United Nations Human Rights Committee in 2011. Revising the Committee's previous General Comment No. 10, it largely encapsulates new developments in international human rights law doctrine – such as the advent of digital ICTs, social media platforms and other technologies that impact expression, and the global trends in state regulation around those issues. As a State party to ICCPR, general comment no. 34 established an interpretative framework for assessing compatibility of domestic legislation with international human rights obligations in Bangladesh.¹²¹

The Committee first highlight that freedom of opinion and expression is one of the essential foundations in a free and democratic society and an indispensable condition for his full development. Suspension of freedom of expression enables transparency, accountability, public interest and the exchange of ideas required for democratic governance. Accordingly, the Committee defines expressive

freedom not just as an individual right but rather essential for securing all human rights.¹²²

General Comment No. 34 confirms that almost any type of expression is protected by Article 19 — political expression, journalism, academic research, artistic expression, communication in the context of culture and religion and commentary on matters of public interest. So, protection is guaranteed not only for information and ideas that are favourably received but also for those that offend, shock or disturb (only) some segments of society.¹²³ This is aligned with the democratic understanding that speech is at the highest value when it defends views that are least accepted, unpopular, or dissenting.

General Comment No. 34 makes one of the most noteworthy contributions through its extensive explanation of the legality requirement. According to the Committee, limitations on expression must be provided for by law and drafted with sufficient precision that individuals can regulate their conduct accordingly. Vague or overly discretionary laws do not meet this requirement, as they fail to provide procedural safeguards against the arbitrary restrictions on protected speech by enforcement authorities. It is especially pertinent to cybersecurity laws, where broadly drafted offences might reach dodgy communication that yields harmful consequences while also capturing regular communication.¹²⁴

Then the necessity principle is somewhat elaborated by the Committee. Any restrictions on expression that are found to be interfering with one of the needful aims recognized by article 19 (3) have to be truly necessary in the sense that it must refer, without exception, every time an aim is fulfilled and start only if no other way exists due a legitimate aim like occupying national security characteristics or public order, harming others rights or moral standings.¹²⁵ It is the government that

¹¹⁹ Constitution of the People's Republic of Bangladesh, art. 39.

¹²⁰ Kaye, *Report of the Special Rapporteur*, paras. 15–28.

¹²¹ UN Human Rights Committee, *General Comment No. 34: Article 19—Freedoms of Opinion and Expression*, CCPR/C/GC/34 (2011).

¹²² Ibid.

¹²³ Ibid.

¹²⁴ Ibid.

¹²⁵ ICCPR, art. 19(3).

appears to bear the heavier burden of showing such a direct and immediate link between the restricted expression and whatever harm it seeks to prevent.¹²⁶ Speculation, political sensitivity, or administrative convenience does not justify restrictions on protected speech.

Another principle significantly tied to necessity is the principle of proportionality. Even for such objective restrictions, General Comment No. 34 requires that the restrictions be none but the least intrusive means of achieving the legitimately pursued objective. A restriction is not in accordance with Article 19 even where it seeks to serve a legitimate aim, and less restrictive means are available. This brings proportionality into play as a protection against potential governmental overreach and ensures that the freedom is the norm and prohibitions are the exception.¹²⁷

Public institutions and government actors must be willing to put up with more criticism than private persons, the Committee states.¹²⁸ Subsidy restrictions intended to protect public officials and agencies from criticism are treated with particular suspicion because they erode democratic oversight and public accountability. In this regard, the Committee does thus not only discourage criminal defamation laws and other measures that could stifle legitimate scrutiny of government conduct.

Particularly relevant in the age of the digital revolution, is General Comment No. 34. Article 19 is expressly applicable to all new forms of communications, including electronic and internet-based technologies. This indicates that the same rights granted to citizens offline must be safeguarded in cyberspace.¹²⁹ Digital expression should NOT be given a lower level of protection just because it (sorta) happens over the internet.¹³⁰ This principle has gained

increased importance as legislation on cybersecurity, misinformation, online extremism and digital surveillance is adopted in multiple states around the world.

General Comment No. 34 serves as detailed guide to assessing the Cyber Security Act 2026, from Bangladesh's perspective. We are particularly concerned about regulatory provisions that use vague language or amount to open-ended surveillance powers (which may conflict with human rights law), preemptive enforcement discretion, and/or punitive consequences disproportionate to harm done — approaches entirely inconsistent with the principles advanced by Committee. Note, international human rights law does not preclude cyber regulation from prospectively applying to all or some subset of Internet communications. Thus, GC 34 plays an important role as a measure against which restrictions on online expression in Bangladesh must be gauged when considering their constitutional and international legality.¹³¹

5.4 Principles of Necessity and Proportionality in Restricting Speech

Under contemporary international human rights law, the principles of necessity and proportionality form the main safeguards against the abuse of restrictions on freedom of expression. And though international legal instruments acknowledge that freedom of expression is not absolute, they prescribe narrowly defined circumstances under which states may intervene in expressive activity. These principles maintain the compatibility of governmental regulation with democratic governance, rather than turning presumptively legitimate regulatory purposes into means of disparaging dissent, criticism, or political participation.¹³²

¹²⁶ General Comment No. 34, paras. 33–35.

¹²⁷ Ibid., para. 22.

¹²⁸ Ibid., para. 38.

¹²⁹ Ibid., para. 12.

¹³⁰ Ibid., paras. 12 and 15.

¹³¹ Cyber Security Act 2026 (Bangladesh), ss 25(1), 31, 44, 52; UN Human Rights Committee, *General*

Comment No. 34: Article 19—Freedoms of Opinion and Expression (2011) CCPR/C/GC/34, paras 22–25, 33–36.

¹³² Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge: Cambridge University Press, 2012), 131–45.

The normative basis upon which these principles rest is found within article 19(3) of the International Covenant on Civil and Political Rights (ICCPR), to apply restrictions on freedom of expression only where those limitations prescribed by law, not arbitrary but when necessary for protecting other rights or reputations, national security interests, public order, health or morals.¹³³ As for the fact that the word “necessary” made it into Article 19, these drafting and interpretive histories show this was chosen as an especially high bar to state interference. No benefit, administrative convenience, or political utility can justify restrictions. Instead, they need to show that there is a clear and urgent social necessity and establish the causal link between the forbidden statement and the risk of harm they try to mitigate.¹³⁴ These claims are reinforced by the case law of the UN Human Rights Committee, which has generally explained that necessity means more than hypothetical risk or global pabulum about public interest. The Committee explained in General Comment No. 34 that limitations shall only be applied for the reasons laid down and should be strictly related to the objective they are based on.¹³⁵ Thus, it is the responsibility of States to show that the interference mitigates real and identifiable risk, rather than theoretical or speculative harms. The necessity aspect of Gunther's proportionality elaborates this in particular by identifying the frequent inability, specific to regulatory interventions related to cybersecurity, in which governments operate by using broad concepts like national security, public order, misinformation or digital harm without demonstrating that expressed words challenged under restriction creates sufficiently severe risks to warrant such curtailment.

The second key principle is that of proportionality, which stipulates that any restriction imposed should be proportionate to the legitimate aim pursued. And where a measure serves a legitimate aim, non-

compliance with international human rights law exists wherever that burden falls disproportionately upon expressive freedom in relation to the harm sought to be remedied.¹³⁶ Thus, proportionality not only serves as a gatekeeper ensuring the right remains intact while allowing regulated action on a limited basis.

Contemporary proportionality analysis typically consists of four cumulative questions. First, the aim of the restriction must be a legitimate objective under international law. Second, the measure has to be rationally linked to the goal. Third, its necessity must be of such a magnitude that there is no less restrictive alternative that would achieve an equivalent degree of protection. Lastly, the advantages created by this restriction must outplay the resulting harm to another right, namely freedom of expression.¹³⁷ The failure at any stage makes the restriction inconsistent with international human rights standards.

Much of the theorizing about proportionality is comparative constitutional jurisprudence. As Aharon Barak puts it, proportionality is a constitutional algorithm for balancing even between conflicting rights and public interests – but also contemplates that governmental action not go further than would be reasonably necessary to achieve the intended goal.¹³⁸ This is because freedom of expression serves an important role in enabling democratic deliberation, governmental accountability, and public participation. Thus, any restrictions on political communication, journalistic work, academic research or other forms of expression that serve a public interest are most deserving of judicial scrutiny.¹³⁹

International and regional courts have continuously used necessity and proportionality analysis in speech-related disputes. The European Court of Human Rights in *Handyside v. United Kingdom*, stated that freedom of expression is applicable to ideas which

¹³³ International Covenant on Civil and Political Rights, adopted December 16, 1966, 999 UNTS 171, art. 19(3).

¹³⁴ Manfred Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary*, 2nd ed. (Kehl: N.P. Engel Publishers, 2005), 462–64.

¹³⁵ United Nations Human Rights Committee, *General Comment No. 34: Article 19—Freedoms of Opinion and Expression*, CCPR/C/GC/34 (2011), para. 22.

¹³⁶ *Ibid.*, para. 34.

¹³⁷ Barak, *Proportionality*, 340–60.

¹³⁸ *Ibid.*, 87–96.

¹³⁹ *Ibid.*, 367–75.

“offend, shock or disturb,” and adding that “such are the demands of pluralism, tolerance and broadmindedness without which there is no democratic society.”¹⁴⁰ The Court also held that any restriction shall conform to a “pressing social need” and must be proportionate to the legitimate aim pursued. In like manner, in *The Sunday Times v. United Kingdom* the Court reiterated that restrictions on freedom of expression must be justified and that the restriction must not go beyond what is necessary in a democratic society.¹⁴¹

In the digital sphere, the idea of necessity and proportionality has taken on new importance. Communication technologies have fundamentally altered the nature of expression—with enormous implications for the scale, speed and extent to which ideas can be disseminated—opening up new opportunities for collective democratic engagement at the same time as generating anxieties over criminal activity, misinformation and hate speech; posing challenges for national security.¹⁴² Many governments tend to respond to these issues pass into laws that grant them with surveillance powers, content-removal mechanisms, regimes of intermediary liability or even criminal sanctions on online activity. These are, of course, valid aims, but international human rights bodies have pointed to the risk that regulation in the digital space will impose overly broad requirements with disproportionate real-life impacts.¹⁴³

The UN Special Rapporteur on Freedom of Opinion and Expression has consistently stated that the same tests required in respect of restrictions impacting off-line communication must also apply to online speech.¹⁴⁴ Similarly the Human Rights Council asserted that government protections of rights individuals have offline must apply online, as there is no basis to conclude that constitutional protection

should carry less weight for digital than it does actual communication.¹⁴⁵ These advances establish that, notwithstanding the increased deployment of technologies by law enforcement and military agencies across the globe, quest for legislative reform has not reasonably altered the core attributes of legality, necessity and proportionality.

The principles serve as a foundation for evaluating the compliance of Cyber Security Act 2026 with human rights in Bangladesh. The laws using imprecise language, indefinite enforcement discretion, intrusive surveillance power or criminal penalties must be analyzed in light of necessity and proportionality. Even when cybersecurity and public order are valid governmental goals, limitations remain only legal if they meet narrow tailoring (i.e., precision), evidence-based requirements, as well as being demonstrably needed to address identifiable harms. Actions that exceed these boundaries may jeopardize not only Article 19 of the ICCPR also the constitutional right to freedom of speech and expression found in Article 39 of the Constitution of Bangladesh.¹⁴⁶

As a result, necessity and proportionality serve as essential checks against regulatory excess. They keep the core concept that freedom of expression is the rule and government suppression an exception, so as to sustain democratic values centered at least in principle around openness, accountability, and public participation in both physical and digital public spheres.

5.5 Worldwide legal jurisprudence on expressions online

Digital communication technologies have expanded rapidly and altered how freedom of expression is exercised, which has forced courts, international tribunals and human rights bodies to rethink

¹⁴⁰ *Handyside v. United Kingdom*, 1 EHRR 737 (1976), para. 49.

¹⁴¹ *The Sunday Times v. United Kingdom*, (1979) 2 EHRR 245, para. 62.

¹⁴² David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/29/32 (2015), paras. 15–28.

¹⁴³ *Ibid.*, paras. 33–39.

¹⁴⁴ *Ibid.*, paras. 51–58.

¹⁴⁵ United Nations Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/RES/32/13 (2016).

¹⁴⁶ Constitution of the People's Republic of Bangladesh, art. 39; ICCPR, art. 19.

orthodoxies about speech regulation. Political debate, civic engagement, and information exchange mainly take place on social media platforms, online news portals, blogs, video-sharing services and encrypted messaging applications. In turn, modern legal thought is increasingly acknowledging that constitutional and human rights guarantees traditionally given to forms of expression should also be offered to digital discourse.¹⁴⁷

Central to global jurisprudence right now is the principle that online speech should be entitled to at least as high a level of protection as offline expression, with the argument that this principle is either debatable or self-evident being flatly rejected. International human rights bodies have recognised that technological change only affects the manner of communication, but not the nature of the substantive right at stake. Thus, to initialize the historical context for this discussion, it is important to note that the Human Rights Committee has reaffirmed explicit recognition of Article 19 on ICTs and all forms of contemporary communications including internet based technologies such as electronic media and any digital platforms in the future.¹⁴⁸ As a result, the imposition of legal restrictions on online expression must meet the same standards of legality, necessity and proportionality as traditional speech.

The *Shreya Singhal v. Union of India* ruling by the Supreme Court of India is one of the landmark judicial pronouncements on issues related to online expression. Section 66A of the Information Technology Act 2000 made it a crime to transmit any information which is deemed "grossly offensive" or just annoying, but the Court struck down Section 66A as unconstitutional.¹⁴⁹ The Court held that the provision was unconstitutional because its language was vague, it gave too much room for enforcement

discretion, and inhibited lawful speech. Importantly, the judgment stated that indeterminate statutes create legal uncertainty and allow for arbitrary limitation on democratic discussions.¹⁵⁰ This ruling has emerged as the most important statement on free speech on the internet and, importantly, for jurisdictions like Bangladesh that confront parallel issues of regulating online content.

The jurisprudence of the United States Supreme Court has also profoundly influenced global understandings of expressive freedom in the digital era. Although many foundational decisions predate the emergence of social media, the constitutional principles they articulate continue to shape contemporary debates. In *Brandenburg v. Ohio*, the Court held that expression may only be restricted where it is directed toward inciting imminent lawless action and is likely to produce such action.¹⁵¹ This demanding test prohibits restrictions of speech founded on indirect or speculative harms, and requires a direct causal link between expression and unlawful conduct.¹⁵² The *Brandenburg* doctrine thus remains a robust protector against government efforts to stifle unpopular or dissenting viewpoints in the name of public order or security concerns.

Likewise, Europe has again provided more of a fundamental form to standards for governing online speech. *Delfi AS v. Estonia* (No 64569/09)(Grand Chamber 16 June 2015) The question before the European Court of Human Rights was whether or not an online news portal can be liable for defamatory comments posted by users.¹⁵³ The Court found liability after examining the specific facts of the case, but acknowledged that access to the internet is necessary to enable democratic debate and disseminate information. The ruling demonstrates the Court's ongoing struggle to reconcile freedom of expression

¹⁴⁷ Molly K. Land and Jay D. Aronson, *New Technologies for Human Rights Law and Practice* (Cambridge: Cambridge University Press, 2018), 42–59.

¹⁴⁸ United Nations Human Rights Committee, *General Comment No. 34: Article 19—Freedoms of Opinion and Expression*, CCPR/C/GC/34 (2011), para. 12.

¹⁴⁹ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

¹⁵⁰ *Ibid*

¹⁵¹ *Brandenburg v. Ohio*, 395 U.S. 444 (1969).

¹⁵² Frederick Schauer, *Free Speech: A Philosophical Enquiry* (Cambridge: Cambridge University Press, 1982), 92–96.

¹⁵³ *Delfi AS v. Estonia*, App. No. 64569/09, Judgment of 16 June 2015.

against competing rights while keeping the internet a venue for public discussion.

In addition, a more recent development was in the case of *Magyar Helsinki Bizottság v. Hungary* where the European Court acknowledged access to information as an essential element of freedom of expression.¹⁵⁴ The Court found that becoming formless and irrelevant in the political realm is more often than not dependent on access to public records of government audiences via digital platforms.¹⁵⁵ Of course, such an interpretation goes beyond the accepted view of expressional freedom (that is, freedom to disseminate and receive information) as it relates to public debate and accountability.

These judicial developments were further underscored by International human rights bodies. Freedom of expression is applicable to internet-mediated communication (General Comment No. 34 para. 43), and requires that cybercrime provisions be precise and not vague, intermediary liability regimes cannot be overbroad, and government powers that limit lawful expression must comply (not only the lawfulness of the measure under international law).¹⁵⁶ The Human Rights Committee, which monitors the implementation of the ICCPR by state parties, has also pointed out that digital communication is essential for democratic participation, journalism, academic inquiry and civic engagement—so restrictions on those must be treated with utmost scrutiny.

A second key aspect of global jurisprudence relates to shutdowns and disruptions of the internet. International human rights mechanisms recognize that blanket shutdowns of Internet access amount to an irreversible violation of freedom of expression, since they have the effect of impeding a broad group from seeking, receiving and imparting information. The

Human Rights Council has consistently condemned measures aimed at deliberately disrupting the flow of information through the internet, calling upon states to refrain from imposing such restrictions save in limited circumstances and only as provided for in international law.¹⁵⁷

The body of comparative jurisprudence is also showing a clear increasing demand for legal certainty and independent scrutiny. Courts have long struck down laws that use vague and subjective terms such as “offensive,” “annoying,” “false,” or “harmful” speech in jurisdictions where there is no objectively developed legal definition for those concepts.¹⁵⁸ Vagueness makes predictability elusive, enables selective enforcement, and creates chilling effects for law-abiding citizens who want to participate in public discourse. Likewise, the erosion of judicial supervision mechanisms meant to safeguard against abuse of surveillance powers, content-removal mechanisms and expeditious digital investigative methods has developed similarly over the years.¹⁵⁹

The global jurisprudence, when taken together, shows that there is a growing international consensus on the need to protect online expression. Courts and human rights institutions are increasingly acknowledging the role that digital communication serves in compelling democratic functions, and thus, requiring the highest levels of constitutional protection. While approaches differ between jurisdictions, a broad framework has emerged that encompasses legality, necessity and proportionality, transparency and judicial accountability.¹⁶⁰

In comparing these developments, by Bangladesh, they provide a compelling reason to consult how we seek to approach the Cyber Security Act 2026. Although comparative decisions are not legally

¹⁵⁴ *Magyar Helsinki Bizottság v. Hungary*, App. No. 18030/11, Judgment of 8 November 2016.

¹⁵⁵ *Ibid.*, paras. 149–56.

¹⁵⁶ Human Rights Committee, *General Comment No. 34*, paras. 24–25.

¹⁵⁷ David Kaye, *Report of the Special Rapporteur on Freedom of Opinion and Expression*, A/HRC/35/22 (2017), paras. 8–15. United Nations Human Rights

Council, Resolution 32/13, *The Promotion, Protection and Enjoyment of Human Rights on the Internet* (2016).

¹⁵⁸ *hrey Singh v. Union of India*, paras. 83–90.

¹⁵⁹ David Kaye, A/HRC/29/32 (2015), paras. 51–58.

¹⁶⁰ ICCPR, art. 19; Human Rights Committee, *General Comment No. 34*, paras. 21–36.

binding, they provide a glimpse into international norms constraining digital expression and illustrate why cybersecurity ends need not come at the expense of enabling a central freedom. Though legislation using loose terms, sweeping intelligence powers, broad executive discretion or heavy-handed criminal sanctions may have been sufficient for yesteryears human rights tests, such laws seem unlikely to clear the low bar of a newly maturing global consensus on legal standards. Accordingly, the legitimacy of cyber regulation does not solely depend on how important or significant (or even compelling) the interest pursued might be viewed, but whether and to what extent the mechanism of regulation is aligned with constitutional (and some international) frameworks that protect free speech in cyberspace.¹⁶¹

6.1 Legislative Context and Goals for the Cyber Security Act 2026

Bangladesh's third legislative twist of the law on digital communication, cyber offences and online expression — the Cyber Security Act 2026 (CSA 2026) — has come into force. This trajectory of regulation is marked by an evolution between responses to advancements in technology, security imperatives and international human rights advocacy whilst enduring continued tension between legitimate cyber governance aims with the countervailing constitutional protections for freedom of expression. The Act was conceived in a new world consisting of accelerated growth in internet penetration, ubiquitous social media, expanded e-commerce activities and widespread digitization of government services.¹⁶² Though these developments raised real issues related to cybercrime and data protection, they also could not do anything but increase the fundamental tensions between national security needs and freedom of speech as secured by Article 39 of the constitution.¹⁶³ There have been three distinct wave of digital era legislations in Bangladesh's regulatory landscape. The first phase began with the enactment of Information

and Communication Technology Act 2006 (ICT Act 2006) which was originally designed for electronic commerce conformation and to punish cyber crime. But the Information and Communication Technology (Amendment) Act 2013 fundamentally changed that legislation, with a vastly broadened section 57 which made it an offence to publish electronic material which was "false" or "obscene," defamatory or prejudicial to law and order. This change imposed vague legislative language with harsh criminal sanctions, allowing for expansive administrative discretion, arbitrary prosecution against journalists, scholars and civil society organizations.¹⁶⁴ The provision also faced widespread criticism for conflating toxic digital behavior with political speech protected by the constitution.

This was followed by the second phase of activism, with the enactment of the Digital Security Act 2018 (DSA 2018) in response to criticism of vagueness surrounding section 57. Many of the substantive provisions that caused controversy retained a modified version of the statutory structure even though the structure was not in keeping with either recent textualist or dynamic interpretation trends. Offences concerning "propaganda", "false information" and "defamation" still used vague wording, while investigators maintained broad powers without any adequate judicial control.¹⁶⁵ One point that Constitutional scholars noted was that the DSA showed legislative continuity instead of real change. The third phase of the process began with the introduction, and subsequent repeal, by Act No. 88 of 2022 (the Cyber Security Act 2026) of a new regulatory architecture in Nigeria replacing that established under the DSA 2018. The Government recognized this Act as a response to new challenges related to cybersecurity threats, cloud infrastructure and foundational digitally-enabled infrastructure. The primary focus of the new legislation was to widen the regulatory net beyond limited "critical information

¹⁶¹ Constitution of the People's Republic of Bangladesh, art. 39; ICCPR, art. 19.

¹⁶² Government of Bangladesh, *Cyber Security Act 2026* (Dhaka: Bangladesh Government Press, 2026).

¹⁶³ Constitution of the People's Republic of Bangladesh, art. 39.

¹⁶⁴ Information and Communication Technology (Amendment) Act 2013 (Bangladesh), s. 57.

¹⁶⁵ Digital Security Act 2018 (Bangladesh), ss. 21, 25, 31.

infrastructure-only" legislations to protect a larger digital ecosystem, because it has now become interdependent and connected.¹⁶⁶ While these objectives constitute legitimate governmental concerns, the Act's provisions employ vague terminology and impose disproportionate criminal penalties that risk violating Article 19 of the ICCPR and Article 39 of Bangladesh's Constitution. Section 31 contains sweeping surveillance powers without judicial oversight; section 44 mandates consecutive prison sentences for broadly defined "cyber terrorism" offences; and section 25(1) outlaws "defamatory online content" without defining key terminology.¹⁶⁷

International and regional human rights bodies, including the United Nations Special Rapporteurs, have repeatedly found that laws concerning cyber terrorism in Bangladesh do not meet internationally recognized standards of lawfulness, necessity and proportionality under Article 19 of the ICCPR. The fact that the legislation frequently has a chilling effect on legitimate participation in public debate rather than addressing strict cybercrime offences demonstrates, between all three phases of legislation there is continuity, not reform, through regulation. Legislative History and the Objectives of the Cyber Security Act 2026.

The third major legislative version of controlling digital communication, cyber crimes and freedom of speech has been enacted in the shape as Cyber Security Act 2026 (CSA 2026) by Bangladesh. That regulatory trend mirrors changing responses to technological progress, security imperatives, and international human rights pressures, tempered by ongoing friction between the legitimate purpose of cyber governance and constitutional protections for freedom of expression. The Act came out in an era of multi-dimensional transformation of our digital landscape with increasing internet penetration, diffusion of social media, rapid digitization in e-commerce and workflow of public administration. Although these

developments raised alarm bells about cyber crime and data protection, they also sharpened underlying tensions between national security interests and the constitutional guarantee of freedom of speech protected under Article 39.

The digital regulatory history of Bangladesh has three legislative phases. The first phase started with the ICT Act 2006 which was mainly enacted to legitimize e-commerce and criminalizing couple of cyber offences. The Information and Communication Technology (Amendment) Act 2013, however, changed the shape of the legislation altogether with an extended version of section 57 which penalised any electronic publication that was found to be "false," "obscene," "defamatory" or "prejudicial to law and order."¹⁶⁸ This Amendment was vague language with concomitant harsh criminal sanctions which allowed for overly broad administrative discretion and arbitrary prosecution to target journalists, academics and civil society actors. The rule drew extensive criticism as unduly conflating dangerous online speech with constitutionally protected political speech.

Phase two started following the introduction of the DSA 2018 (Digital Security Act 2018), which was in response to increasing criticism about section 57 being too vague. Many of the substantive provisions that previously created controversy were incorporated in modified forms notwithstanding the changed statutory structure. Broad definitions of "propaganda," "false information" and "defamation" remained, investigative authorities had extensive powers without meaningful judicial oversight.¹⁶⁹ Some constitutional experts claimed that the DSA was "business as usual," not real reform.

Phase three began with the introduction of a new regulatory framework by the Cyber Security Act 2026 that replaced DSA 2018. The Act is introduced by the Government with certain emerging challenges against such areas mentioned within the stand of cyber

¹⁶⁶ Government of Bangladesh, *Cyber Security Act 2026*, ss. 3, 31, 44.

¹⁶⁷ Cyber Security Act 2026 (Bangladesh), ss. 25(1), 31, 44.

¹⁶⁸ Information and Communication Technology (Amendment) Act 2013 (Bangladesh), s. 57.

¹⁶⁹ Digital Security Act 2018 (Bangladesh), ss. 21, 25, 31.

security threats, cloud infrastructure and digitally foundational infra zones. Legislation extended reach beyond "critical information infrastructure-only" focused regulation to include a combination of protection across digital ecosystem.¹⁷⁰ These aims are valid concerns of government, but the Act use broad terms and imposes an excessive punishment that may infringed upon Article 19 of ICCPR and Article 39 of Constitution Bangladesh. In particular, section 31 provides for the most extreme form of surveillance powers with no judicial oversight; section 44 mandates mandatory prison for a range of irrationally vague crimes termed "cyber terrorism"; and section 25(1) again libels loosely defined acts as "defamatory online content".¹⁷¹

International human rights organisations and UN Special Rapporteurs have stated time and again that the cyber laws in Bangladesh do not meet with international standards of legality, necessity and proportionality, as implemented through Article 19 of the ICCPR.¹⁷² Proceeds of International Terrorism Act 2002, which criminalises certain trade in media and violent/salacious literature to restrict or censor the non-violent activities of civil society.¹⁷³

6.2 Definitions, Scope of Digital Expression and Related Offences

6.2.1 Statutory Definitions

At bottom, the constitutional legitimacy of cybercrime legislation relies on the precision with which the conduct in question is statutorily defined. Legislative certainty is a requirement of the rule of law in criminal law: people can only regulate their conduct, if they understand what conduct is prohibited. This becomes increasingly important in the context of digital expression as online communication also includes political, journalistic, academic and personal activity. Vague wording in legislation threatens to punish

public speech that would otherwise be legal, alongside truly malicious action, with the inevitable consequence of deterring legal behavior and chilling constitutionally-protected activity.¹⁷⁴

To bolster the capability to combat against cybercrime, Cyber Security Act 2026 was announced in Bangladesh. Because the Act repeals the Digital Security Act 2018, however many conceptual underpinnings remain intact. The definitions of cyber offences incorporated in the law and attached systems are many. Although these provisions may look to modernise Bangladesh's existing framework for cyber regulation, a closer inspection shows that a number of definitions are still too wide, giving enforcement authorities significant (though uncontrolled) discretion in interpretation with little attributable legal rough casing.¹⁷⁵

This difficulty is illustrated by the definition of cybersecurity. Instead of limiting the model to protect computer systems from unauthorized access or interference by technological means, the framework uses broad language that can include a wide range of online activities. This becomes constitutionally problematic to the extent that vague concepts without a clear legal standard for what will bestow criminal liability are involved. International human rights jurisprudence requires that criminal law legislation which places restrictions on free expression be written in clear and foreseeable terms.

Section II: DefinitionsThe Act also takes broad definitions of digital data, computer system and digital platform. Although these provisions are a reflection of the technological reality that digital communication occurs across interconnected systems, their combined width represents an immense widening of criminal liability. All but every type of Internet-based

¹⁷⁰ Government of Bangladesh, *Cyber Security Act 2026*, ss. 3, 31, 44.

¹⁷¹ Cyber Security Act 2026 (Bangladesh), ss. 25(1), 31, 44.

¹⁷² David Kaye, *Report of the Special Rapporteur on Freedom of Opinion and Expression*, A/HRC/29/32 (2015), paras. 15–58.

¹⁷³ Human Rights Watch, *Bangladesh: Repeal Repressive Digital Security Act* (New York: Human Rights Watch, 2023), 5–8.

¹⁷⁴ Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge: Cambridge University Press, 2012), 131–45.

¹⁷⁵ Government of Bangladesh, *Cyber Security Act 2026*, ss. 2–5.

communication is within the statute. As a result, the Act expands government control of an extraordinarily wide range of expressive conduct.¹⁷⁶

Notably, this is especially Martin GBF problematic where the statutory definitions touch on offences that impinge upon freedom of expression. Some of these contain concepts like false information, propaganda or defamatory content with no defined legal standards. These speech-based definitions rely on subjective interpretation, unlike cyber offences such as hacking or identity theft that can be quantitatively measured. And because there are no clear standards, it leaves us unclear about where political speech ends and crime begins.¹⁷⁷

However, on the constitutional level, vague statutes do not meet the legality principle that requires criminal laws to be defined with sufficient precision. It is reflected in international human rights law in Article 19 (3) of the ICCPR, which allows restrictions upon expression only when they are "provided by law." The interpretation of the Human Rights Committee is that the law must be published and not give unbounded discretion to administrative authorities.¹⁷⁸

Comparative jurisprudence reinforces this position. The Supreme Court of India struck down Section 66A of THE INFORMATION TECHNOLOGY ACT with the reason that expressions such as "grossly offensive" had no objective legal meaning (Shreya Singhal v. Union of India).¹⁷⁹ The Court noted that the imprecision of such terms is always going to lead to a chilling effect by discouraging people from legitimate expression in fear of prosecution.¹⁷⁹

6.2.2 Coverage and Corruption Related to Online Expression

¹⁷⁶ Government of Bangladesh, *Cyber Security Act 2026*, ss. 2–5. United Nations Human Rights Committee, *General Comment No. 34*, para. 25.

¹⁷⁷ Government of Bangladesh, *Cyber Security Act 2026*, ss. 25, 31, 44.

¹⁷⁸ United Nations Human Rights Committee, *General Comment No. 34*, para. 25.

The definitional framework of the Act is built out in section 2 of the CSA 2026, by using expansive language around cyber related crimes that increases power over offences much broader than the common narrow definitions of what constitutes a cyber offence. Cybersecurity is defined in these statutes without any distinction between actual security threats and protected speech under the First Amendment.¹⁸⁰ This allows regulators to treat indecent utterances as cybersecurity issues that they can prosecute for criminal punishment.

The Act covers any electronic means of communication, such as posts on social networks / digital media or news on the internet and messaging application messages. Section 3 of the new law specifically applies to "digital information infrastructure," including cloud services and third-party operational models. This turns the Act from a bare infrastructure protection regime into full-scale regulation of digital expression.¹⁸¹

Meanwhile, section 25(1), which criminalizes the promulgation of "defamatory online content," has used vague terminology that has no objective legal foundation.¹⁸² The exemption doesn't distinguish between speech harshly criticizing public officials (protected under the Constitution) and false statements made against individuals that could harm them. Because the language is vague, it effectively allows for arbitrary enforcement against journalists and civil society organizations.

While Section 29 lays out punishment for "false information" threatening national security, that harm need not be demonstrated. The vague wording of the provision does not fulfill the legality requirement imposed by Article 19 (3) ICCPR. This law can be

¹⁷⁹ David Kaye, *Report of the Special Rapporteur on Freedom of Opinion and Expression*, A/HRC/29/32 (2015), paras. 15–28.

¹⁸⁰ Government of Bangladesh, *Cyber Security Act 2026*, s. 2.

¹⁸¹ Government of Bangladesh, *Cyber Security Act 2026*, s. 3.

¹⁸² Cyber Security Act 2026 (Bangladesh), s. 25(1).

used to suppress genuine whistleblowing and political criticism, under the fig-leaf of national security.¹⁸³

Thirdly, section 44 prescribes mandatory prison terms for cyber terrorism (use of digital systems to intimidate the public).¹⁸⁴ This overly broad definition sweeps in constitutionally protected political activity—spanning from peaceful protests to social media critique of government policy. The compulsory penalty contravenes the proportionality standard under General Comment No. 34.¹⁸⁵

The various offences within the Act demonstrates a specific concern around regulatory overreach by distorting the line between serious crimes in cyberspace (cyber offences) and expression that is protected under constitutions. This becomes a new form of structural tensions existing between cyber regulation and expressive freedom as witnessed by Bangladesh's earlier ICT Act 2006.¹⁸⁶

6.3 powers of investigation and enforcement authorities

The CSA 2026 thus also confers extraordinarily broad powers on investigative authorities to snoop and collect digital communications, with little effective judicial oversight.¹⁸⁷ The provision permits the Commissioner of Cybersecurity to obtain access to electronic devices, intercept communications, and require internet service providers to provide users' information under written authorization. These powers do not use court orders or independent oversight systems, allowing for wholesale surveillance.

Section 32 empowers investigators to seize electronic devices, and cryptography can be decryption of communications by the assistive tools by forensic without any demonstration of probable cause.¹⁸⁸

Section 35 forces technology companies to release user data within seventy-two hours after a written demand, with no option for judicial review. These provisions also establish an extensive system of surveillance infrastructure for the preemptive monitoring of digital expression.¹⁸⁹

Section 38 authorizes the enforcement authorities to prevent or restrict access to online content considered prejudicial to national security without a judicial order in advance.¹⁹⁰ Content-control mechanism for every little thing comes up—and prevents censorship that is in violation of Article 19 which prohibits routine restrictions.

It requires mandatory information-sharing among public and private sectors, meaning it would need tech firms to provide user data if asked by the government. This violates privacy rights, and Section 40 then punishes non-compliance—effectively forcing tech companies to work as surveillance contractors without adequate protections.¹⁹¹

Section 43 introduces expedited data preservation powers allowing investigators to compel the retention of digital communications without having to demonstrate that ongoing investigation is taking place.¹⁹² Section 46 authorizes the use of information obtained for purposes other than the initial investigation without a proportionality analysis.¹⁹³

The Act contains no independent oversight mechanisms for its enforcement framework. The internal review committee is mandated under section 48 will be completely composed of government officials, without any independent members or civil

¹⁸³ United Nations Human Rights Committee, *General Comment No. 34*, para. 25.

¹⁸⁴ Cyber Security Act 2026 (Bangladesh), s. 44

¹⁸⁵ United Nations Human Rights Committee, *General Comment No. 34*, para. 34.

¹⁸⁶ ^ Ridwanul Hoque, "Freedom of Expression and Constitutional Adjudication in Bangladesh," *Asia-Pacific Journal on Human Rights and the Law* 24, no. 2 (2023): 145–68.

¹⁸⁷ Government of Bangladesh, *Cyber Security Act 2026*, s. 31.

¹⁸⁸ Cyber Security Act 2026 (Bangladesh), s. 32.

¹⁸⁹ Cyber Security Act 2026 (Bangladesh), s. 35.

¹⁹⁰ Cyber Security Act 2026 (Bangladesh), s. 38.

¹⁹¹ Cyber Security Act 2026 (Bangladesh), s. 40.

¹⁹² Cyber Security Act 2026 (Bangladesh), s. 43.

¹⁹³ Cyber Security Act 2026 (Bangladesh), s. 46.

society representation.¹⁹⁴ This internal mechanism does not provide adequate external oversight in the very governance institution exercising surveillance powers.

International human rights bodies emphasise that surveillance measures which directly or indirectly restrict the right of expression must meet the high standards under Article 19(3) of legality, necessity and proportionality.¹⁹⁵ The UN Special Rapporteur notes that such blanket surveillance powers without judicial review violate these requirements as they put an unjustifiable burden on expression. The CSA 2026's surveillance framework does not meet these standards and therefore imposes chilling effects that contradict the protection of fundamental rights established under Article 39 of the constitution.

6.4 Due Process Considerations Procedure Safeguards

Cyber security legislation is not just a matter of substantive offences; it requires procedural safeguards governing investigatory, prosecutorial, and adjudicatory processes. International human rights law recognizes that limitations to freedom of expression and can only be justified where individuals are guaranteed appropriate procedure to protect them against the arbitrary action of the state. Due process acts as one of the cornerstones that gives rise to the rule of law and embodies legality, fairness, transparency in compliance with objective principles & thereby using judicial functions as a bulwark against arbitrary action.¹⁹⁶

The Cyber Security Act 2026 boosts investigatory powers considerably yet provides relatively sparse procedural safeguards. Law enforcement agencies are permitted to investigate and access digital data, take

stampings and imprints of electronic devices, capture lower types of electronic evidence only at levels that seriously infringe or encroach upon privacy rights and freedom of speech. Cybercrime investigations often need prompt action, however international standards demand that monitoring powers should be subject to independent judicial review and effective legal remedies.¹⁹⁷

Section 31 provides blanket surveillance powers without any judicial warrant, allowing investigatory agencies to breach on electronic device solely with written approval of government officials—flouting Article 35 of the Bangladesh Constitution which mandates procedural due process. The Act even raises issues of the right to fair trial in criminal matters involving online speech. At the same time, residential police coercion limits may venture against, rather than further, legal secure rights — looser investigative scope constrained by harsh felonies can create apprehensions surrounding exercising process or impugning government conduct. If criminal offences are framed in broad terms, individuals may not be able to know if their online behaviour is caught by the prohibitions, thus undermining the requirement of legal certainty that is one of the building blocks of what constitutes due process.¹⁹⁸

Under Section 35, technology companies are required to provide data on users within seventy-two hours of a request in writing, with no right for judicial review or the user seeking notification. The lack of advance, meaningful notice to impacted individuals (and the absence of an opportunity to contest exposure) in notifying affected data subjects is contrary to basic elements of procedural due process under international law. Except to the extent that a judicial authority issues an order prohibiting or subjecting the exercise of these

¹⁹⁴ Government of Bangladesh, *Cyber Security Act 2026*, s. 48.

¹⁹⁵ United Nations Human Rights Committee, *General Comment No. 34*, para. 22.

¹⁹⁶ ICCPR, arts. 14, 19; UN Human Rights Committee, *General Comment No. 34*, CCPR/C/GC/34 (2011), paras. 21–25.

¹⁹⁷ David Kaye, Report of the Special Rapporteur on Freedom of Opinion and Expression, A/HRC/29/32 (2015), paras. 51–58; European Court of Human Rights, *Roman Zakharov v. Russia*, App. No. 47143/06 (2015).

¹⁹⁸ Constitution of the People's Republic of Bangladesh, art. 35; Manfred Nowak, U.N. Covenant on Civil and Political Rights: CCPR Commentary (2nd ed., Mannheim: Engel Publishers, 2005), 462–68.

powers to prior scrutiny, Section 38 enables enforcement authorities to impede or entirely restrict access to online content, constituting preventive censorship devoid of oversight by any other means than post-deprivation review.

The Act provides for no timelines dictating how long data should be retained and when it is to be destroyed, creating a continuing system of data retention facilitating back-end analysis of digital expression without a requirement to show an active investigation. Investigators are given the power to retain digital communications without judicial oversight under Section 43, and information obtained in support of investigations may subsequently be misused for purposes outside of those in which it was originally collected (Section 46) without needing to conduct a proportionality analysis.

Under section 48, the Cybersecurity Department shall have an internal review committee that consists of government officials only, and which does not include independent members or any judicial representation nor civil society. The review body cannot offer truly effective oversight because it functions within the bureaucratic structure that has been given surveillance authority. The Human Rights Committee of the UN has noted that independent internal review mechanisms are a prerequisite for meeting the legality requirement under Article 19(3).¹⁹⁹

The procedural architecture within the Cyber Security Act 2026 should be viewed against both Articles 39 of Bangladesh's Constitution and Article 19 of ICCPR, these reviews indicate a clear superiority of enforcement mechanisms over institutional safeguards. A more muscular legislative framework that provides for judicial scrutiny, greater candor, tighter evidential standards, and wider access to effective relief from state action would supplement existing legal protections.

¹⁹⁹ UN Human Rights Committee, General Comment No. 34, para. 25; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

²⁰⁰ Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge: Cambridge University Press, 2012), 340–60.

6.5 The Chilling Effects of Online Speech and Freedom of Expression

A major constitutional critique of the Cyber Security Act 2026 is on how it may deter lawful speech. Legislation creates a chilling effect when it causes people to avoid exercising their protected rights for fear of prosecution, the ambiguity of the law, or other disproportionate legal consequences. Even in areas where prosecutions remain relatively rare, the threat of criminal liability may lead to self-censorship by individuals and groups participating less freely in public life, dampening democratic participation and restricting the marketplace of ideas.²⁰⁰

The International Human Rights Law recognizes protection of freedom of expression not only for the popular ideas but also combating any criticism of public authorities, government policy or views held by other minorities. Therefore, laws around digital communications must avoid creating a climate in which individuals are afraid to engage in legitimate expression due to ambiguity about the legal lines.

Many provisions of the Cyber Security Act 2026 are capable of generating such a chilling effect. The broad inclusion of online publication activities in the offence, coupled with very serious

6.6 Overbroad, Vague, and Criminalized Speech

Overbreadth and vagueness are among the most prominent doctrines in constitutional law under which courts consider freedom of expression questions. Both doctrines seek to prevent legislation from imposing vague legal standards or overly expansive criminal prohibitions on protected speech. When the statutory texts do not clearly define what kind of conduct is prohibited, they compromise legal certainty, encourage capricious enforcement and have extremely chilling consequences for democratic activism.²⁰¹

International human rights law predicates that all restrictions on expression "be provided by law" [33],

²⁰¹ ICCPR, art. 19; UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34 (2011), paras. 24–25.

in the sense that the norm must be publicly accessible, foreseeable and phrased with enough precision to allow an average person to conduct himself. Laws using vague terms like "false," "offensive," or "prejudicial" without an objective legal standard are not sufficient to achieve this goal, because individuals cannot adequately ascertain the outer bounds of lawful speech.²⁰²

Under these principles, the Cyber Security Act 2026 raises several important questions. The criminalization of "defamatory online content" in Section 25(1) is an imperfect example of overbreadth, as it defines serious defamatory falsehoods affecting private reputation not only seriously damaging false statements about public officials but broadly protected criticism of public officials. The problem with the law is that it reaches far too broad, touching real political discussion as well as defamation.

Even broader is section 29's ban on "false information" connected to national security, which criminalises expression beyond what is reasonable, as it does not require proof of real harm or intent. The indecisively worded provision does not satisfy the legality requirement under Article 19(3): No one can be reasonably forewarned as to what would amount to 'false information' which is prohibited.

Third, Section 33's criminal prohibition of "cyber propaganda" detrimental to national security is overbroad by targeting legitimate political expression in addition to harmful disinformation efforts. Instead of drawing a line between political speech that is protected by the Constitution and true incitement, it merely lumps them all together.

By capturing actions traditionally protected political expression such as peaceful protests in pursuit of democratic reform, Section 44 becomes an overly broad weapon targeting legitimate political activity against unavoidable prison sentences for "cyber

terrorism," defined by its use of digital systems to intimidate or create fear among the public. The mandatory penalty violates the deferential applicability requirement under General Comment No. 34, as it takes no account of context, intent or actual harm caused by the expression in question.

The broad terms used in the Act breach the vagueness doctrine, as they do not create clear legal standards for identifying behaviour that makes one criminally liable. The vague construction in Sections 25(1) of "defamatory online content," Section 29's "false information," Section 33's "cyber propaganda" and even less so witheach vague, subjective term like cyber terrorism.²⁰³

The definitional framework of the CSA 2026 continues raising serious constitutional issues through overbreadth and vagueness. While the definitions of "cybersecurity" and even "digital information infrastructure" are somewhat covered under the Act, these terms are still far too expansive and leave significant interpretative leeway to whatever enforcement agency would deploy them without providing definitive legal guidelines or rules on what constitutes a breach or violation. This ambiguity raises the question of what separates political expression protected by this promise from conduct that entails liability, and it affords opportunities for uneven application of the law or even a chilling effect on privileged speech.

Overcriminalization presents an additional concern. Criminal penalties are the most invasive form of state control and should be used only as a last resort. International standards favour civil remedies, administrative regulation or focused enforcement means by which to sanction expression-related conduct in preference to imprisonment. Over-reliance on criminal law might well turn cyber regulation from a tool of public protection to a tool of speech control.²⁰⁴

²⁰² UN Human Rights Committee, General Comment No. 34, para. 25; Manfred Nowak, U.N. Covenant on Civil and Political Rights: CCPR Commentary (2nd ed., Mannheim: Engel Publishers, 2005), 462–68.

²⁰³ Shreya Singhal v. Union of India, (2015) 5 SCC 1, paras. 83–94.

²⁰⁴ David Kaye, Report of the Special Rapporteur on Freedom of Opinion and Expression, A/HRC/29/32 (2015), para. 51.

When taken together, vague drafting and overly broad offences coupled with harsh criminal sanctions violate the doctrine of legality, necessity and proportionality under Article 19 of the ICCPR, which is mirrored in Article 39 of Bangladesh Constitution itself. In our view, legislative reform must ensure that statutory drafting is precise and offences narrowly defined; so that independent judicial oversight and proportionate sanctions distinguish real cybercrime from speech that should be protected expression.²⁰⁵

VII. COMPARATIVE AND JURISPRUDENTIAL INSIGHTS

7.1 Examples of Attempts by the United States to Regulate Digital Speech

The First Amendment, which provides the absolute protection of expression with little room for regulation, is at work in the most speechprotective approach to digital regulation used by countries such as the United States. I03: Federal government cannot infringe speech content unless meets highest constitutional burden of strict scrutiny (compelling interest, narrowly tailored restriction).²⁰⁶ Cited By 1 This has led the U.S. The classic case in point for this analysis is *Reno v. ACLU* when the Court struck down parts of the Communications Decency Act that made it a crime to transmit "indecent" and "patently offensive" online material, because they found the Internet to be a forum for democratic discourse deserving protection.²⁰⁷

Section 230 provides sweeping immunity to online platforms against third-party content, in stark contrast with mandatory intermediaries liability in Bangladesh under the Cyber Security Act 2026. In the United States, speech inciting lawless action is governed by the *Brandenburg v. Ohio* test, which holds that expression must be directed to inciting imminent lawless action and likely to produce such action.²⁰⁸

This high standard does not permit justifying bans based on speculative harms. The overbreadth doctrine allows general challenges to laws that restrict in a suboptimal manner protected speech, and the vagueness doctrine lets someone argue that sufficient precision is needed to give fair warning.²⁰⁹ This means both doctrines could potentially strike down undefined terms in the Cyber Security Act 2026, such as "defamatory online content," "false information" and "cyber propaganda".

7.2 The EU digital rights landscape and the Digital Services Act

EU follows a rights-balancing between the freedom of expression and privacy²¹⁰ Digital SafetyThe EU Charter of Fundamental Rights Article 11. The Digital Services Act (DSA) came into force in 2022 and consists of harmonised rules for digital services with the establishment of single obligations within the EU market for all online services providers offering their services on the European single market.²¹¹

DSA imposes tiered obligations on digital services, applying stricter rules to larger platforms or those with more societal impact. Some key goals are the protection of users against illegal content while also ensuring the fundamental rights of freedom of expression and information, transparency in content moderation and effective oversight guarantees.²¹² Mandatory content moderation transparency reporting, and disclosure of algorithmic recommendation means.

Enforcement flows both ways: coordination at national level through the Digital Services Coordinators for platforms in their respective territories, but also at European level for Very Large Online Platforms (VLOPs).²¹³ It is noteworthy that the DSA's balancing of illegal content in Article 14 requires member states to respect "the right to a fair

²⁰⁵ Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge: Cambridge University Press, 2012), 340–60.

²⁰⁶ First Amendment to the United States Constitution.

²⁰⁷ *Reno v. ACLU*, 521 U.S. 844 (1997).

²⁰⁸ *Brandenburg v. Ohio*, 395 U.S. 444 (1969).

²⁰⁹ *Grayned v. City of Rockford*, 408 U.S. 104 (1972).

²¹⁰ Charter of Fundamental Rights of the European Union, art. 11.

²¹¹ Regulation (EU) 2022/2065 (Digital Services Act).

²¹² European Commission, *Digital Services Act: keeping us safe online* (2025).

²¹³ Eurojust, *Digital Services Act factsheet* (2024).

trial and due process rights protecting information, including as applicable standards for notice and removal", whereas Section 38 of the Cyber Security Act 2026 contains administrative character content-blocking without any judicial oversight.²¹⁴

7.3 The IT Act in India and Protective Shadows of Judiciary

Given our shared constitutional traditions combined with the common challenges posed by vague cyber legislation and issues of national security, India offers the most pertinent comparative precedent against which to measure Bangladesh. *Shreya Singhal v. Union of India* is a landmark case which strikes down Sec 66A of Information Technology Act 2000 i.e. transmitting information that is "grossly offensive," "annoying" or causing "inconvenience".²¹⁵

The Supreme Court held that the formulation in Section 66A was vague, arbitrary and gave wide discretion to the authorities enforcing it and had a chilling effect on free speech.²¹⁶ The Court stated that vague statutory language is a threat to legal certainty and creates the potential for arbitrary oppression of democratic political debate. Three constitutional tests were applied to the extent of Section 66A, and it was struck down because terms like "grossly offensive" and "annoying" are devoid of objective legal meaning.²¹⁷

India, which amended its IT Act in a 2013 exercise, retained the substantive offences imposed by Section 66A but proscribed them through more flexible language as Sections 67 and 67A (obscene information; false or misleading electronic communication) – another demonstration of legislative continuity echoing the fate which befell Bangladesh in transitioning from the ICT Act 2006 to Digital Security Act (DSA) 2018 to Cyber Security Act (CSA) [2026].²¹⁸

7.4 Lessons and transfer principles for Bangladesh
From comparative jurisprudence, five transferrable principles for reforming Bangladesh's cyber legislation:

This is Statutory Drafting, Principle 1: Precision
Legislation should consist of predictable language with legally-binding criteria. The ambiguously drafted laws in the Cyber Security Act 2026 against "defamatory online content," "false information," "cyber propaganda" and "cyber terrorism" must replace with narrow categorisation of offences.²¹⁹

Principle 2: Values of an Independent Judicial Authority to Oversee the Use of Surveillance and Content

Prior judicial approval is needed for surveillance that impacts expression and limits on content. Judicial redress mechanisms have to be built into Section 31's warrantless surveillance, along with other ways to enhance legislative scrutiny in Section 38's administrative content-blocking.

Third Principle) Criminal Sanctions have to be proportional

Context, intent and tangible harm must be considered in deciding who faces criminal penalties. Comment No. 34: The prohibition on more severe penalties is a violation of proportionality requirements under section 44.

Principle 4: Independent Oversight Mechanisms

The internal Cybersecurity Department review committee in Section 48 must be substituted with independent judicial or multi-stakeholder oversight, including civil society.

Principle 5: Criminalizing Cybercrime versus Protected Expression

Legislation should unmistakably distinguish real cybercrime from constitutionally-protected political expression. This distinction was underscored in the *Shreya Singhal* decision, which struck down the provisions that ensnared legitimate discourse.²²⁰

²¹⁴ UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34 (2011), para. 23.

²¹⁵ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

²¹⁶ *Shreya Singhal v. Union of India*, paras. 83–94.

²¹⁷ *Shreya Singhal v. Union of India*, para. 87.

²¹⁸ Information Technology Act 2000 (India), ss. 67, 67A.

²¹⁹ Constitution of the People's Republic of Bangladesh, art. 39; ICCPR, art. 19.

²²⁰ *Shreya Singhal v. Union of India*, para. 90.

7.5 Jurisprudential Trends in Constitutional Review of Cyber Legislation

Constitutional review of cyber legislation is shaped by three converging jurisprudential trends:

Trend 1. Rejected Lower Protection for Online Speech
Most importantly, international human rights institutions invariably dismiss the argument that online speech deserves less protection than it would as an offline form of expression. The Human Rights Committee ruled that Article 19 applies to all forms of modern communication, including internet-based technologies.

New trend 2: Chilling Effect Doctrine.

Courts are recognizing chilling effects as signifiers of overbroad restrictions more than ever before. As the *Shreya Singhal* decision made clear, vague terms are chilling because individuals self-censor to avoid indecisive prosecution.

Trend 3: Reinforced Procedural Safeguards

Independent judicial review, transparency and effective remedy for surveillance and content-control measures is an increasing requirement in jurisprudence. According to the UN Human Rights Committee, internal review mechanisms that are not independent in terms of functions or personnel do not meet the legality requirement under Article 19(3)

The convergence of these trends leads to five basic requirements for broadly legitimate cyber laws: (1) precise statutory definitions; (2) judicial review of intrusive measures; (3) proportionate sanctions in context; and (4) independent oversight; each at all levels, and with evidentiary burdens put expressly on the government side of the equation or more protective side depending on how much dispute you have got in your constitution regarding expression versus protecting society from things like cybersecurity intrusions; (5) a clear definition of protected speech as it relates to topics available via these channels without its subliminal imagery. (6) —> How do

authorities distinguish between criminal behaviour undertaken online versus what might generally be subject to some imperatives? The Cyber Security Act 2026 fails all five criteria, meaning it must be amended to comply with the Constitution: specifically Article 39 and ICCPR Article 19.²²¹

VIII. REFORM AGENDA

8.1 Legislative reform: going narrow on offences and clear on terms

State must undertake comprehensive law reform to bring provisions as in Cyber Security Act 2026 in line with norms enshrined within the constitutional guarantees under Article 39 and International obligations as envisaged within the ICCPR Article 19. This necessitates that the criminal offence be drafted with enough precision to allow an individual to foresee the legal consequences, in fulfilment of the legality requirement of Article 19(3).²²²

The criminalisation of "defamatory online content" found in Section 25(1) must be repealed and replaced with narrowly defined offences which delineate between valid criticism of public officials protected by the Constitution, on the one hand, and harmful false statements about facts on the other. It is this provision that currently catches legitimate political discourse alongside defamation in all forms.²²³

All offences in section 29 must be replaced by offences requiring proof of actual harm, malicious intent and direct-connection to a national security offence therefore making the prohibition of "false information" dealing with matters affecting national security pursuant to section 29 contrary to Articles 19(2) and (3) of the ICCPR.²²⁴ Instead of broadly criminalizing "cyber propaganda," as in Section 33, manifesto proposals must only genuinely and demonstrably harm-motivated disinformation campaigns with clearly defined offences establishing intent to cause harm, making clear the difference

²²¹ UN Human Rights Committee, General Comment No. 34, para. 25.

²²² UN Human Rights Committee, General Comment No. 34: Article 19—Freedoms of Opinion and Expression, CCPR/C/GC/34 (2011), para. 25.

²²³ Cyber Security Act 2026 (Bangladesh), s. 25(1).

²²⁴ Cyber Security Act 2026 (Bangladesh), s. 29.

between constitutionally protected political discourse and genuinely damaging propaganda.²²⁵

Section 44's mandatory five-year prison sentences for "cyber terrorism" should be repealed as these penalties violate the proportionality requirement found in General Comment No. 34 (Articles 19 and 20) which requires greater nuance to take account of context and intent, and actual harm done.²²⁶ The definition must be further honed to require a direct link to imminent unlawful action per the test laid out in *Brandenburg v. Ohio*.²²⁷ The provisions concerning definitions of "cybersecurity" and "digital information infrastructure" under the Act should be substituted with unambiguous terms that offer criteria to reasonably determine whether the legal conditions are met.

8.2 Enhancing judicial supervision and independence of the review mechanism

Surveillance and content-control powers in the Cyber Security Act 2026 operate without independent judicial review, compromising procedural due process standards imposed by Article 35 of Bangladesh's Constitution as well as legal standards under ICCPR Article 19(3).²²⁸

Eliminate surveillance powers of Section 31 that work without automatic judicial warrants where law enforcement or intelligence agencies can access data from electronic devices, communicate by intercepting in real time, and collect stored information from nearby cloud services only with prior written authorisation from an independent and impartial judicial authority.²²⁹ In *Roman Zakharov v. Russia*, the Court went on to state that any law providing for surveillance that affects private communications must be such as to secure prior judicial approval.²³⁰

Judicial orders should be obtained first to empower enforcement authorities to block, remove or restrict access to online content. Independent judicial oversight or at least multi-stakeholder, including civil society representation must replace the Cybersecurity Department's internal review committee in charge of Section 48.²³¹

The data retention framework in sections 43 and 46, which allows for open-ended retention of information should be amended so that judicial authorization is required where information is to be retained, that there are mandatory timelines around the destruction of data once it has been obtained, and such obtained information cannot be used for purposes other than those of the original investigation without a proportionality analysis.²³²

8.3 Strengthening Procedural Safeguards and Due Process

Others are baseless rule regarding the enforcement of the provisions of Cyber Security Act 2026. Due process serves the purpose of the rule of law by making sure all stages in the criminal justice system maintain legality with fairness, transparency and judicial accountability.²³³

The expedited data disclosure regime of Section 35, which mandates companies to disclose user data within seventy-two hours under written request without the possibility of judicial review or advance notice to affected individuals, must be amended accordingly: affected individuals should receive at least notification about the government requests directed towards them, opportunities for contestation against such orders and access to remedies—core elements of procedural due process under international law.²³⁴

²²⁵ Cyber Security Act 2026 (Bangladesh), s. 33.

²²⁶ Cyber Security Act 2026 (Bangladesh), s. 44.

²²⁷ *Brandenburg v. Ohio*, 395 U.S. 444 (1969).

²²⁸ Constitution of the People's Republic of Bangladesh, art. 35.

²²⁹ UN Human Rights Committee, General Comment No. 34, para. 22.

²³⁰ European Court of Human Rights, *Roman Zakharov v. Russia*, App. No. 47143/06 (2015).

²³¹ UN Human Rights Committee, General Comment No. 34, para. 25.

²³² *Roman Zakharov v. Russia*, para. 23.

²³³ UN Human Rights Committee, General Comment No. 34, para. 21.

²³⁴ ICCPR, art. 2(3).

The Act should include transparency requirements on content moderation decisions, which would require enforcement authorities to justify blocking of content, including written explanations for orders restricting the placing of content, information about the legal ground underlying a restriction of pluralistic media (e.g. Member States should specify if national security or another ground has been invoked) and specifying how long the content will be removed. This is in line with transparency reports conducted under the EU DSA.

Those subject to content-blocking orders should have recourse to independent courts for effective review of executive action within reasonable time frames. Article 2 (3) of the ICCPR frames a right to effective remedies for violations of rights whereas judicial mechanisms should be accessible and abuse prevented.

Accused persons should maintain various procedural rights during criminal proceedings, such as the right to obtain legal counsel, challenge evidence against them and protection from self-incrimination; this too must be made a make-or-break aspect of the Act. The Act should provide clear norms regulating collection, preservation, authentication and admissibility of electronic evidence.

8.4 Protecting Digital Rights and Transparency

Explicit digital rights protections and transparency mechanisms denoting adequate safeguards from operational misuses should be integrated in a reformed Cyber Security Act 2026, securing constitutional guarantees as envisaged under Article 39 especially with respect to ICCPR article 19.²³⁵ Digital Rights Charter which should be enshrined in the Act with a clear recognition that online expression deserves equal protection, and opposition to the view that speech on digital media must face lesser constitutional protections than conventional speech.²³⁶

²³⁵ Constitution of the People's Republic of Bangladesh, art. 39; ICCPR, art. 19.

²³⁶ UN Human Rights Committee, General Comment No. 34, para. 12.

²³⁷ Regulation (EU) 2022/2065 (Digital Services Act), art. 27.

Freedom of expression: The Act should require technology platforms operating in Bangladesh to disclose any algorithmic recommendation mechanism that may influence which content is prioritized (algorithmic governance can silence lawful expression on a systematic scale, with no transparency). It is in compliance with the EU DSA which requires platforms to share algorithms used for recommendations.²³⁷ The Act should require annual public reporting on key enforcement statistics, including the number of content-blocking orders obtained, the number of surveillance warrants authorized under Section 21, the number of criminal prosecutions brought under this part and the status/outcomes of judicial review. Such transparency bolsters public confidence while maintaining balance between security goals and civil liberties.

There is need to have multi-stakeholder digital rights committee (including civil society organisations, technology companies, academic experts and human rights advocates) which will ensure that the Act work as intended.²³⁸

Aligning Cyber Legislation in Bangladesh with Global Human Rights Norms

Reform agenda of the Cyber Security Act 2026 must be built around compliance with international human rights standard ICCPR Article 19 (requirements of legality, necessity and proportionality) and domestic constitutional guarantees in Bangladesh under Article 39.²³⁹ Comparative jurisprudence provides five fundamental requirements for constitutionally-compliant cyber legislation:

Requirement 1: Precise Statutory Definitions

Legislation must use precise, predictable terms and legal standards. Outdated and broadly worded provisions within Cyber Security Act 2026 must be replaced with narrowly defined offences creating a notice of fair warning and standards of enforceability.²⁴⁰

²³⁸ UN Human Rights Committee, General Comment No. 34, para. 26.

²³⁹ ICCPR, art. 19.

²⁴⁰ UN Human Rights Committee, General Comment No. 34, para. 25.

Satisfy condition 2 with respect to intrusive measures:
Judicial oversight

Expression and content-blocking surveillance must be conducted only with prior judicial authorisation. Sections 31 and 35 require mechanisms for judicial oversight of warrantless surveillance while Section 38 must incorporate mechanisms to prevent or compel administrative content-blocking.²⁴¹

CONTEXT-BASED SANCTIONS 3: Sanctions must be proportionate

Criminal laws need to reflect context, intent, and real-world harm. The problem of mandatory penalties under Section 44 as a violation of proportionality in accordance with General Comment No.34²⁴²

Requirement 4: Independent Oversight Mechanisms

Non-independent internal review committees do not satisfy legality standards. Replace the internal review committee under Section 48 with independent oversight by a judge or mixed expert-multi-stakeholder body containing civil society representatives.²⁴³

Criteria 5 — Make a clear distinction between cybercrime and protected expression

We must apply legislation that separates actual cybercrime from constitutionally protected political speech. This distinction was underscored in the *Shreya Singhal* decision which had struck down provisions that interfered with even legitimate discourse. This distinction is not met by the overbroad provisions in the Cyber Security Act 2026.²⁴⁴

Bringing the Cyber Security Act 2026 in line with these emerging precepts would improve not just constitutional governance under Article 39 but also reassure Bangladesh's compliance, as a state party to ICCPR Article 19; cybersecurity concerns cannot

justify abandoning constitutional guarantees of freedom of expression.²⁴⁵

IX. CONCLUSION

9.1 Summary of Findings

This holistic unbundling of the Bangladesh Cyber Security Act 2026 demonstrates an intrinsic constitutional misalignment with Article 39 of the Constitution as well as international obligations by virtue of ICCPR Article 19. The overly-broad and vague provisions of the Act which criminalize "defamatory online content," "false information," "cyber propaganda" or any form of cyber terrorism violate the legality limit under Article 19(3) as individuals are unable to foresee what conduct is prohibited.

Sections 31-36 of the surveillance framework allow secret access to an individual's device and communication traffic without a judicial warrant, merely based on the authorization of government officials the seniority of whom is not specified in the law. The lack of judicial review undermines procedural due process principles under Article 35 of the Constitution of Bangladesh, and legality principles under ICCPR Article 19(3).

The Act chills online speech and free expression on a massive scale; it stops many from exercising their constitutional right to engage in political discussion for fear of prosecution. The open-ended nature of the broad provisions you propose rely on abstract concepts, could be arbitrarily applied in violation of the requirement of legal certainty which is a necessary element of due process.

What comparative jurisprudence from the U.S. First Amendment, EU Digital Services Act and Indian Supreme Court *Shreya Singhal* case reveals is that effective cyber regulation can be valuable without

²⁴¹ UN Human Rights Committee, General Comment No. 34, para. 22; ICCPR, art. 2(3).

²⁴² UN Human Rights Committee, General Comment No. 34, para. 22.

²⁴³ UN Human Rights Committee, General Comment No. 34, para. 25.

²⁴⁴ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, para. 90.

²⁴⁵ Constitution of the People's Republic of Bangladesh, art. 39; ICCPR, art. 19.

over-criminalizing online speech. The best legal systems separate true cybercrime from legitimate democratic expression, take targeted approaches to curtailing it, and include independent judicial review and strong procedural protections.

We analysed the Cyber Security Act 2026 from a constitutional law, international human rights law and comparative jurisprudence perspective in this study. Current cyber laws have to find a middle ground between safeguarding digital security and maintaining fundamental constitutional rights. The results suggest that many provisions of the Act do not strike the right balance, allowing for wide administrative discretion which could result in arbitrary application or potentially deter journalists, academia, civil society human rights defenders and ordinary citizens from engaging in open discourse on democratic issues.

9.2 Compatibility check: constitutional and international standards

The Act carries with it failure against all five cumulative test for constitutionally permissible cyber legislation as demarcated under Article 19(3) of ICCPR and Article 39 of Bangladesh's Constitution.

Legality Requirement

The lack of accessibility, foreseeability and the vagueness requirement means that the Act fails this element of legality. The use of “defamatory online content” in Section 25(1), and false information in Section 29, “cyber propaganda” under Section 33, as well as “cyber terrorism” under Section 44 are also actionable without objective legal meaning to aid enforcement and create chilling effects on protected expression.

Legitimate Purpose Requirement

Cybersecurity is a valid government interest, but the Act ventured beyond meaningful decision trigger areas and into infringing upon protected political speech. The Act makes no attempt to differentiate between malicious disinformation, bona fide public political debate, responsible journalism or serious scholarship.

Necessity Requirement

When submitting to the necessity requirement, the Act falls short, as even if law enforcement has never found

a less-beacon-based criminal sanction that meets cybersecurity goals, it ought not be necessary. More recent scholarship shows that international human rights bodies are increasingly concerned about the “over-chilling” problematic nature of any criminal sanctions on defamation. Less restrictive alternatives would be available in the form of civil remedies or administrative sanctions.

Proportionality Requirement

The Act violates the proportionality requirement as mandatory prison sentences of five years (Section 44) for this new crime of “cyber terrorism” do not consider context, intention or an actual harmful effect on behaviour. The square penalty would infringe the proportionate requirements in General Comment No. 34 and prevent a court from taking account of any mitigating factors.

Procedural Safeguards Requirement

The procedural safeguards requirement of the Act fails, because mechanisms for independent judicial approval and oversight of surveillance and content-control powers are not provided; transparency mechanisms do not exist to provide an overview on their use; nor effective remedies to remedy abuses. Section 48 internal review committee is not independent and does not meet the legality requirement under ICCPR Article 19(3).

The key question here is if the Cyber Security Act 2026 adheres to the constitutional rights in Bangladesh and also with international human rights obligations. Building upon the previous analysis, The answer is qualified not absolutes. All of the goals are in general accordance with a legitimate government objective as recognized in both domestic and international law. However, some of the legislative measures taken to them are inconsistent with established constitutional and international law standard for restrictions on free expression.

9.3 Final Supporting Elements and Potential Directions for Reform

To reform the Cyber Security Act 2026 in a manner that is in line with constitutional and international norms, India must reform its legislation around these five principles:

Principle 1: Precise Statutory Definitions

Clear and predictable terms with clear legal standards should be used in legislation. The Cyber Security Act 2026 must get rid of vague provisions and require definite nasty offences that can be proven to have actually caused harm, occur with proof of intentions to commit a crime, and be directly linked causally to an identified national security threat; they should offer fair warning that actions during legal exercise or which are incidental will not make people liable and adequate standards for law enforcement.

Principle 2: Judicial oversight of invasive measures
Prior judicial authorization by an independent and impartial judiciary is a necessity for surveillance that impede the right to freedom of expression, as well as content-blocking. Section 31's content-blocking and warrantless surveillance by Section 38 must be changed to require those actions to receive a judicial order, as the European Court of Human Rights decided in the case *Roman Zakharov v. Russia*.

Principle 3: Context-Sensitive Proportionate Sanctions
Punishments cannot be undifferentiated; they need to take into consideration circumstances, intention, and actual harm. Proportional sanctions should replace mandatory penalties under Section 44, allowing civil remedies or administrative sanctions for expression-related conduct where criminal penalties disproportionate under General Comment No. 34.

Principle 4: Independent Oversight Mechanisms
Independent, though. Internal review committees — those are not independent at all and therefore fail legality requirements. The committee to review the alleged derogatory practice of Section 48 has to be replaced with independent judiciary oversight or multi-stakeholder oversight — incorporating civil society representation — to ensure accountability prevents investigation based on political motivation.

Principle 5: Making a clear and public distinction between cybercrime and legitimate expression

Legislation has to differentiate real cybercrime against constitutionally protected political activity. This recognition was crucial in the *Shreya Singhal* decision which struck down provisions that would fail to draw the line between illegal content and lawful speech. However, many provisions of the Cyber Security Act

2026 are too wide and would fail this distinction, making criminals out of speech that critics and journalists would want to engage in for legitimate democratic purposes.

Pathways for Reform

The Cyber Security Act should contain an interpretation clause that refers expressly to international human rights standards. Therefore, ambiguous provisions should be interpreted consistently with ICCPR Article 19, General Comment No.34 and the comparative constitutional jurisprudence. The Act should also provide for a Digital Rights Charter (which is conventionally included in such legislation) with an explicit affirmation that online expression would be protected on the same basis as offline expression.

In the end, we should look to a rights-based model of cybersecurity reform that views digital security and freedom of expression as complementary values rather than competing ones. A legally sourced, adequate and balanced legal arrangement rooted in legality, necessity and proportionality with transparent regulations and judicial oversight that addresses cybersecurity issues in Bangladesh will not only maximize public confidence in constitutional governance guaranteed by Article 39 but also compliance of ICCPR Article 19.

The results show that sound reform can be about more than cherry-picking statutory amendments; it is ultimately a matter of embedding a comprehensive rights-based model within cyber governance. Bangladesh has a critical opportunity to rewill¹⁹¹ its approach to cyber regulation in a way that both enhances national cybersecurity and protects constitutional democracy.

Author Contributions:

Emon Hossain Bijoy; Conceptualization, methodology, literature review, investigation, and drafting of the manuscript. Md. Atikur Rahman Ranga; Conceptualization, legal and constitutional analysis, methodology, investigation, critical analysis, drafting, and substantial revision of the manuscript. Md. Nazmul Hasan; Literature review, legal research, comparative analysis, data collection, and drafting of relevant sections. Mst. Erfana Fairuj Anisa;

Investigation, literature review, analysis of relevant legal and policy materials, interpretation of findings, and manuscript editing. Md. Shadin; Legal research, comparative research, data verification, manuscript review, and revision. All authors contributed to the development of the research, critically reviewed the manuscript, approved the final version, and agreed to be accountable for the content of the work.

REFERENCES

A. International Treaties and International Instruments

- [1] *Constitution of the People's Republic of Bangladesh*. Articles 35, 39.
- [2] *International Covenant on Civil and Political Rights*. Adopted December 16, 1966. 999 UNTS 171.
- [3] United Nations. *Universal Declaration of Human Rights*. GA Res. 217A (III). UN Doc. A/810 (1948).
- [4] United Nations Human Rights Committee. *General Comment No. 34: Article 19—Freedoms of Opinion and Expression*. CCPR/C/GC/34. Geneva, 2011.
- [5] United Nations Human Rights Council. *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. A/HRC/RES/32/13. Geneva, 2016.
- [6] United Nations Human Rights Council. *The Right to Privacy in the Digital Age*. A/HRC/RES/29/22. Geneva, 2015.
- [7] United Nations Human Rights Council. *The Right to Privacy in the Digital Age*. A/HRC/RES/34/7. Geneva, 2017.
- [8] United Nations Human Rights Council. *The Right to Privacy in the Digital Age*. A/HRC/RES/42/15. Geneva, 2019.

B. Bangladesh Legislation

- [9] *Cyber Security Act 2026* (Bangladesh). Sections 2–5, 25(1), 29, 31–36, 38, 43, 44, 46, 48.
- [10] *Digital Security Act 2018* (Bangladesh).
- [11] *Information and Communication Technology Act 2006* (Bangladesh).
- [12] *Information and Communication Technology (Amendment) Act 2013* (Bangladesh).

C. Cases

Bangladesh

- [13] *Anwar Hossain Chowdhury v. Bangladesh*, 41 DLR (AD) 165 (1989).

India

- [14] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1. Paras. 83–90, 87–94.

United States

- [15] *Brandenburg v. Ohio*, 395 U.S. 444 (1969).
- [16] *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).
- [17] *Packingham v. North Carolina*, 582 U.S. 98 (2017).
- [18] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
- [19] *Grayned v. City of Rockford*, 408 U.S. 104 (1972).

European Court of Human Rights

- [20] *Delfi AS v. Estonia*, App. No. 64569/09, Judgment of June 16, 2015.
- [21] *Handyside v. United Kingdom*, 1 EHRR 737 (1976).
- [22] *Magyar Helsinki Bizottság v. Hungary*, App. No. 18030/11, Judgment of November 8, 2016.
- [23] *Roman Zakharov v. Russia*, App. No. 47143/06 (2015).
- [24] *The Sunday Times v. United Kingdom*, (1979) 2 EHRR 245.
- [25] *Cumpănă and Mazăre v. Romania*, App. No. 33348/96 (2004).

D. European Union Legislation

- [26] European Parliament and Council. *Digital Services Act*. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. *Official Journal of the European Union*.

- [27] *Charter of Fundamental Rights of the European Union*. Article 11 – Freedom of expression and information.
- [28] *European Convention on Human Rights (ECHR)*. Article 10 – Freedom of expression.

E. Books

- [29] Barak, Aharon. *Proportionality: Constitutional Rights and Their Limitations*. Cambridge: Cambridge University Press, 2012.
- [30] Bhatia, Gautam. *Offend, Shock, or Disturb*. New Delhi: Oxford University Press, 2016.
- [31] Donnelly, Jack. *Universal Human Rights in Theory and Practice*. 3rd ed. Ithaca: Cornell University Press, 2013.
- [32] Land, Molly K., and Jay D. Aronson. *New Technologies for Human Rights Law and Practice*. Cambridge: Cambridge University Press, 2018.
- [33] Nowak, Manfred. *U.N. Covenant on Civil and Political Rights: CCPR Commentary*. 2nd ed. Kehl: N. P. Engel Publishers, 2005.
- [34] Schauer, Frederick. *Free Speech: A Philosophical Enquiry*. Cambridge: Cambridge University Press, 1982.
- [35] Stone, Geoffrey R., et al. *Constitutional Law*. 8th ed. New York: Wolters Kluwer, 2018.

F. Journal Articles

- [36] Hannum, Hurst. "The Status of the Universal Declaration of Human Rights in National and International Law." *Georgia Journal of International and Comparative Law* 25 (1996): 287–397.
- [37] Hoque, Ridwanul. "Freedom of Expression and Digital Regulation in Bangladesh." *Asia-Pacific Journal on Human Rights and the Law* 24, no. 2 (2023): 145–168.
- [38] *Human Rights Law Review* 12, no. 4 (2012): 627.

G. United Nations Reports

- [39] Kaye, David. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*.

A/HRC/29/32. Geneva: United Nations Human Rights Council, 2015.

- [40] Kaye, David. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. A/HRC/35/22. Geneva: United Nations Human Rights Council, 2017.

H. NGO and Institutional Reports

- [41] Amnesty International. *Repackaging Repression: The Cyber Security Act and Continuing Restrictions on Dissent in Bangladesh*. London: Amnesty International, 2024.
- [42] ARTICLE 19. *The Global Principles on National Security and the Right to Information (The Tshwane Principles)*. London: ARTICLE 19, 2013.
- [43] ARTICLE 19. *Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance*. London: ARTICLE 19, 2014.
- [44] Human Rights Watch. *Bangladesh: Repeal Repressive Digital Security Act*. New York: Human Rights Watch, 2023.
- [45] International Commission of Jurists. *Digital Expression and Human Rights*. Geneva: International Commission of Jurists, 2020.
- [46] ICT International Centre (ICNL). *Bangladesh's Cyber Security Act: A Guide for Civil Society, Media and Humanitarian Organizations*. November 2024.
- [47] Media Defence. *The Right to Freedom of Expression under International Law*. London: Media Defence, 2022.
- [48] Office of the United Nations High Commissioner for Human Rights (OHCHR). *The Right to Privacy in the Digital Age*. 2018.

I. Online Academic Resources

- [49] Council of Europe. *Convention on Cybercrime (Budapest Convention)*. 2001. Articles 14–21.
- [50] Election.com Law. *Information Technology Act 2000 (India)*. Sections 66A (repealed), 67, 67A.

- [51] Global Freedom of Expression. "General Comment No. 34." Columbia University. <https://globalfreedomofexpression.columbia.edu>
- [52] Global Freedom of Expression. "Online Expression Jurisprudence." Columbia University. <https://globalfreedomofexpression.columbia.edu>
- [53] Office of the United Nations High Commissioner for Human Rights. "Universal Declaration of Human Rights." <https://www.ohchr.org>
- [54] Office of the United Nations High Commissioner for Human Rights. "Freedom of Opinion and Expression." <https://www.ohchr.org>
- [55] OHCHR. "Article 19 of the ICCPR." 2020. <https://www.ohchr.org/sites/default/files/Documents/HRBodies/CCPR/GC37/ARTICLE19.docx>
- [56] Organization of American States (OAS). "Special Rapporteurship for Freedom of Expression." 2009. <https://www.oas.org/en/iachr/expression/showarticle.asp?artID=435&IID=1>
- [57] Oxford University Press. *Human Rights Law Review*. 12, no. 4 (2012): 627–72. <https://academic.oup.com/hrlr/article/12/4/627/628921>
- [58] Stanford Law School, Wilson International Programme on Law and Democracy (WILMAP). "General Comment No. 34 on Article 19 of the ICCPR." 2018. <https://wilmap.stanford.edu/entries/general-comment-no-34-article-19-international-covenant-civil-and-political-rights>
- [59] Bangladesh Laws. "সাইবার সুরক্ষা অধ্যাদেশ, ২০২৫ (Cyber Security Ordinance 2025)." <http://bdlaws.minlaw.gov.bd/act-details-1538.html>
- [60] CMS Law. "Digital Services Act: A new legal framework for the platform economy." 2021.
- [61] Eurojust. "Digital Services Act factsheet." 2024. <https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-digital-services-act-factsheet-2024-en.pdf>
- [62] European Commission. "The Digital Services Act package." 2026. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>
- [63] European Commission. "Digital Services Act: keeping us safe online." 2025. https://commission.europa.eu/news-and-media/news/digital-services-act-keeping-us-safe-online-2025-09-22_en
- [64] People of Internet. "Bangladesh's Cyber Protection Act 2026 Ratifies the Old Speech Code." 2026. <https://www.peopleofinternet.com/articles/bangladesh-s-cyber-protection-act-2026-ratifies-the-old-spec.html>
- [65] Scribd. "Overbreadth and Vagueness in Law." 2025.
- [66] Cornell Law School. "Procedural Matters and Freedom of Speech: Vagueness." 2023.