© JMSR 2025 ‖ P-ISSN: 3107-1325 ‖ E-ISSN: 3107-1333 www.jmsrbd.com

Journal of Multidisciplinary Studies and Research
Volume 1, Issue 2, 2025
Indexed Journal
Peer Reviewed Journal

Cyber Crime Legislation in Bangladesh and India: A Critical Analysis

Shahinur Rahman[1]
PhD Scholar
Faculty of Law
Mangalayatan University, India

Dr. Shoeb Ali[2]
Assistant Professor
Institute of Legal Studies and Research
Mangalayatan University, Aligarh, India

ABSTRACT

The exponential growth of digital technology has fundamentally altered social interaction, governance, commerce, and communication in South Asia. Bangladesh and India, as two rapidly digitizing developing nations, have witnessed remarkable progress in internet penetration, digital financial services, and e-governance. However, this digital transformation has also intensified cybercrime, including financial fraud, identity theft, hacking, online harassment, misinformation, and cyber-enabled terrorism. This article critically examines the cybercrime legislative frameworks of Bangladesh and India, focusing on Bangladesh's Information and Communication Technology Act 2006, Digital Security Act 2018, and Cyber Security Act 2023, alongside India's Information Technology Act 2000, the Information Technology (Amendment) Act 2008, and the Digital Personal Data Protection Act 2023. Employing doctrinal and comparative legal methodologies supported by secondary data from government reports, international organizations, and judicial interpretations, the study evaluates legislative effectiveness, enforcement mechanisms, and human rights implications. The analysis reveals that although both countries have enacted relatively comprehensive cyber laws, persistent challenges remain due to vague statutory provisions, inadequate enforcement capacity, lack of specialized judicial infrastructure, and limited regional cooperation. The paper argues that cybercrime governance must move beyond punitive legislation and adopt a holistic approach incorporating legal harmonization, institutional strengthening, digital literacy, and regional collaboration. The study concludes that sustainable cyber governance in South Asia requires a balanced framework that ensures security while safeguarding constitutional freedoms and human rights.

Keywords: Cybercrime, Cyber Law, Bangladesh, India, Digital Security, Comparative Law, Cyber Governance.

1. Introduction

The twenty-first century is characterized by unprecedented digital transformation, reshaping economic systems, governance models, and social interaction. Digital technologies have become integral to development strategies, particularly in South Asia, where governments actively promote digital inclusion and technology-driven growth (UNODC, 2024).

Bangladesh and India exemplify this transition through expansive digital infrastructure, mobile internet connectivity, and digital financial ecosystems. According to the Bangladesh Telecommunication Regulatory Commission, Bangladesh had over **130 million internet subscribers** by late 2024, driven largely by mobile broadband expansion and government initiatives such as "Digital Bangladesh" (BTRC, 2024). India, by contrast, has crossed **900 million internet users**, positioning itself as one of the world's largest digital economies (Telecom Regulatory Authority of India (TRAI, 2024). Digital platforms have facilitated financial inclusion, online education, telemedicine, and e-governance, significantly contributing to socio-economic development.

However, the rapid digitization of society has also expanded opportunities for cybercrime. Cyber offenses threaten national security, economic stability, public trust, and individual privacy. The anonymity, transnational nature, and technological complexity of cybercrime pose unique challenges to traditional criminal justice systems (UNODC, 2024). Recognizing these threats, both Bangladesh and India have enacted cybercrime legislation to regulate digital conduct and protect cyberspace. Nevertheless, concerns persist regarding enforcement effectiveness, misuse of legal provisions, and compatibility with constitutional rights such as freedom of expression and privacy. This article undertakes a comparative and critical analysis of cybercrime legislation in Bangladesh and India to assess whether existing legal frameworks adequately address contemporary cyber threats.

2. Conceptual and International Legal Framework

Cybercrime lacks a universally accepted definition, but it is generally understood as criminal conduct carried out through or against computer systems and digital networks (UNODC, 2021). Scholars often categorize cybercrime into three broad groups: crimes against computer systems, cyber-enabled traditional crimes, and content-related offences (Brenner, 2019).At the international level, the Budapest Convention on Cybercrime (2001) remains the most comprehensive legal instrument, emphasizing procedural safeguards, proportionality, and cross-border cooperation. Although neither Bangladesh nor India is a party to the Convention, its principles are frequently used as a normative benchmark in comparative legal studies (Council of Europe, 2001). International human rights law, particularly the International Covenant on Civil and Political Rights (ICCPR), also plays a critical role in shaping cybercrime regulation. Any restriction on digital expression or surveillance must satisfy legality, necessity, and proportionality standards (UN Human Rights Committee, 2011). These principles form the analytical framework for the present study.

3. Cyber Crime Legislation in Bangladesh

3.1 Legislative Evolution

Bangladesh first addressed cybercrime through the Information and Communication Technology (ICT) Act 2006, later amended in 2013 to introduce harsher penalties and non-bailable offences. The Act criminalized hacking, unauthorized access and electronic fraud but was widely criticized for vague language and excessive executive discretion (Rahman, 2018).In 2018, the Digital Security Act (DSA) replaced key provisions of the ICT Act. While the DSA expanded the scope of cyber offences, including digital defamation and online "propaganda," it also intensified concerns regarding freedom of expression and arbitrary enforcement (Amnesty International, 2022). Responding to domestic and international criticism, Bangladesh enacted the Cyber Security Act 2023, later followed by further legal revisions in 2024–2025. Despite nominal reforms, many substantive provisions of the DSA were retained, leading scholars to describe the reform process as largely cosmetic (Khan, 2024).

3.2 Substantive and Procedural Issues

Bangladesh's cybercrime laws suffer from over-criminalization and vague drafting. Terms such as "hurting religious sentiment" or "damaging the image of the state" lack precise legal definition, enabling broad interpretation by law enforcement agencies (Rahman, 2018). Procedurally, the absence of strong judicial oversight in investigation and arrest processes raises serious due process concerns. Studies indicate that cybercrime laws have been disproportionately used against journalists and political critics rather than organized cybercriminal networks (Amnesty International, 2022).

4. Cyber Crime Legislation in India

4.1 Information Technology Act 2000

India's primary cybercrime statute, the Information Technology (IT) Act 2000, was among the earliest in South Asia. Amended in 2008, the Act criminalizes hacking, identity theft, cyber terrorism, and online fraud, while also establishing institutional mechanisms such as the Computer Emergency Response Team (CERT-In) (Singh, 2020).Unlike Bangladesh's laws, the IT Act provides relatively clearer offence definitions and incorporates intermediary liability frameworks. Judicial interpretation has further strengthened constitutional safeguards, particularly after the Supreme Court struck down Section 66A for violating freedom of speech (Shreya Singhal v. Union of India, 2015).

4.2 Digital Personal Data Protection Act, 2023

A major development in India's cyber legal landscape is the Digital Personal Data Protection Act (DPDP) 2023, which establishes principles of consent, purpose limitation, and accountability in data processing. Although not a cybercrime statute per se, the DPDP Act significantly strengthens privacy protections and complements criminal enforcement (Bhandari, 2024).

4.3 Enforcement and Institutional Capacity

India has invested in specialized cybercrime units, national reporting portals, and digital forensic capacity. While enforcement challenges persist particularly in rural areas the overall framework reflects gradual institutional maturation (NCRB, 2023).

5. Cybercrime Scenario in Bangladesh

Bangladesh has experienced a sharp increase in cybercrime incidents alongside digital expansion. In 2024, more than **13,000 cybercrime complaints** were registered, primarily involving online fraud, harassment, identity theft, and mobile financial scams (CID Bangladesh, 2024).

Mobile financial services such as **bKash** and **Nagad** have become major targets for phishing and SIM-swap frauds (BTRC, 2024). Studies indicate that youth and women constitute the majority of victims, reflecting gaps in digital literacy and awareness (Digital Security Agency, 2024).

Despite legislative reforms, enforcement remains constrained by limited forensic facilities, shortage of trained investigators, and procedural delays.

6. Cybercrime Scenario in India

India faces one of the highest volumes of cybercrime globally. The National Crime Records Bureau reported over **70,000 cybercrime cases in 2024**, marking a continued upward trend (NCRB, 2024).

Financial fraud, identity theft, cyber stalking, and misinformation campaigns are prevalent. While India has established cybercrime reporting portals and specialized cyber cells, enforcement capacity varies significantly across states (NCRB, 2024).

7. Weaknesses and Challenges

Despite the presence of comprehensive cybercrime legislation in both Bangladesh and India, several structural, legal, and institutional weaknesses continue to undermine effective cybercrime governance. These challenges are multidimensional, involving legislative ambiguity, enforcement deficits, human rights concerns, jurisdictional barriers, and systemic judicial limitations.

7.1 Ambiguity and Over breadth of Legal Provisions

One of the most significant weaknesses in cybercrime legislation in both countries is the presence of vague and overly broad statutory language. In Bangladesh, provisions under the ICT Act 2006 and the Digital Security Act 2018 were widely criticized for lacking precise definitions of offenses such as “false information,” “defamation,” and “threats to national security,” which created scope for arbitrary application (Government of Bangladesh, 2018). Although the Cyber Security Act 2023 sought to address some of these concerns, ambiguity persists regarding discretionary powers of law enforcement agencies (UNODC, 2024).

Similarly, in India, certain provisions of the Information Technology Act 2000 particularly those relating to offensive online content and intermediary liability have been criticized for inconsistent interpretation and selective enforcement (NCRB, 2024). Such ambiguity undermines legal certainty and weakens public trust in cyber laws.

7.2 Enforcement Capacity and Institutional Constraints

Both Bangladesh and India face acute shortages of trained cybercrime investigators, digital forensic experts, and specialized prosecutors. Cybercrime investigations require advanced technical expertise, yet law enforcement agencies often lack adequate training and modern forensic infrastructure (CID Bangladesh, 2024; NCRB, 2024). In Bangladesh, cyber forensic laboratories are limited in number and concentrated in major cities, resulting in delays in evidence collection and case processing. In India, although institutional mechanisms such as CERT-In and state cyber cells exist, enforcement capacity varies significantly across states, creating uneven access to justice (NCRB, 2024).

7.3 Human Rights and Freedom of Expression Concerns

Cybercrime laws in both countries have raised serious concerns regarding freedom of expression, press freedom, and privacy. Bangladesh’s Digital Security Act 2018 was frequently criticized by international organizations for being used against journalists, academics, and political activists (UNODC, 2024). Although the Cyber Security Act 2023 reduced the number of non-bailable offenses, concerns remain about misuse of cyber laws to suppress dissent.

In India, cyber laws have occasionally been employed to initiate cases against online critics and whistleblowers, raising questions about proportionality and constitutional safeguards under Articles 19 and 21 of the Indian Constitution (Government of India, 2023).

7.4 Cross-border Jurisdictional Challenges

Cybercrime is inherently transnational. Offenders often operate across borders, making investigation and prosecution extremely complex. Both Bangladesh and India face difficulties

in securing electronic evidence from foreign jurisdictions due to the absence of robust mutual legal assistance treaties and harmonized cybercrime frameworks in South Asia (Council of Europe, 2001).

Bangladesh's non-accession to the Budapest Convention further limits international cooperation, while India's partial alignment has not yet translated into seamless cross-border enforcement (UNODC, 2024).

7.5 Judicial Delays and Procedural Limitations

Judicial systems in both countries struggle with delays in cybercrime adjudication. The lack of specialized cybercrime courts and limited judicial familiarity with digital evidence contribute to prolonged trials and low conviction rates (CID Bangladesh, 2024; NCRB, 2024). Procedural bottlenecks and backlog of cases further erode deterrence and public confidence.

8. Findings

This study reveals several critical insights into the nature, scope, and effectiveness of cybercrime legislation in Bangladesh and India. First, it becomes evident that legislative philosophy differs substantially between the two jurisdictions. Bangladesh's cybercrime framework has evolved through frequent statutory changes, reflecting a reactive and often politically driven approach rather than a stable, principle-based regulatory model. In contrast, India's framework demonstrates gradual doctrinal development supported by constitutional jurisprudence and institutional continuity.

Second, legal certainty and precision emerge as a major point of divergence. Bangladesh's cybercrime statutes, particularly the Digital Security Act 2018 and its successor legislation, contain broadly framed and indeterminate offence definitions. Such vagueness undermines the principle of legality, which requires criminal laws to be precise and foreseeable. Empirical evidence and human rights reports indicate that these provisions have been selectively enforced, disproportionately affecting journalists, activists, and online dissenters rather than sophisticated cybercriminal networks. This pattern weakens public trust in cyber governance and raises concerns about the instrumentalization of cyber law for non-criminal regulatory objectives.

Third, the study finds that procedural safeguards remain insufficient in Bangladesh. Arrest without warrant, limited judicial oversight during investigation, and the absence of specialized cybercrime courts collectively compromise due process guarantees. These deficiencies are inconsistent with international human rights standards, particularly those articulated under the ICCPR, which emphasize necessity, proportionality, and effective remedies.

In India, the findings suggest a comparatively more balanced and institutionally mature framework, though not without shortcomings. The Information Technology Act 2000, supplemented by judicial interpretation, has benefited from constitutional scrutiny, most notably through the invalidation of Section 66A. This jurisprudential intervention has strengthened freedom of expression online and established an important precedent for rights-based cyber regulation. Furthermore, the Digital Personal Data Protection Act 2023 represents a significant normative shift toward privacy protection, addressing a long-standing gap in India's cyber governance architecture.

However, the study also finds that enforcement capacity remains a persistent challenge in India. Despite advanced legal frameworks and institutional mechanisms, uneven implementation across states, limited digital forensic expertise, and difficulties in cross-border cybercrime investigation continue to constrain effective enforcement. These limitations highlight that legislative sophistication alone does not guarantee regulatory success.

Finally, at a regional and international level, both Bangladesh and India exhibit limited alignment with global cybercrime cooperation frameworks. Neither country has fully integrated international best practices relating to mutual legal assistance, transnational evidence sharing, or harmonized procedural safeguards. This gap significantly undermines their capacity to address cybercrime, which is inherently transnational in nature.

9. Recommendations

To address the identified weaknesses and enhance cybercrime governance, the following recommendations are proposed:

9.1 Legal Reform and Clarification

Cyber laws should be revised to ensure precise definitions of offenses, clear procedural safeguards, and proportional penalties. Bangladesh should consider aligning its cybercrime framework with international instruments such as the Budapest Convention, while India should further harmonize intermediary liability and content regulation provisions (Council of Europe, 2001; UNODC, 2024).

9.2 Institutional and Enforcement Capacity Building

Both countries must invest in specialized cybercrime units equipped with modern forensic laboratories and trained personnel. Regular training programs for police, prosecutors, and investigators are essential to keep pace with evolving cyber threats (CID Bangladesh, 2024; NCRB, 2024).

9.3 Protection of Human Rights

Cybercrime legislation must explicitly incorporate safeguards for freedom of expression, press freedom, and privacy. Independent oversight mechanisms should be established to prevent misuse of cyber laws against journalists, researchers, and political opponents (UNODC, 2024).

9.4 Judicial Specialization

The establishment of specialized cybercrime courts with trained judges is crucial to ensure speedy trials and effective adjudication. Judicial capacity-building programs focusing on digital evidence and cyber forensics should be institutionalized (NCRB, 2024).

9.5 Digital Literacy and Public Awareness

Governments should launch nationwide digital literacy and cyber security awareness campaigns targeting vulnerable groups, particularly youth and women. Cyber security education should be integrated into school and university curricula (Digital Security Agency, 2024).

9.6 Regional and International Cooperation

A SAARC-level cybercrime cooperation mechanism should be developed to facilitate intelligence sharing, joint investigations, and mutual legal assistance. Bilateral agreements with technologically advanced jurisdictions should also be strengthened (Council of Europe, 2001).

10. Conclusion

Cybercrime legislation occupies a critical intersection between technology, security, and fundamental rights. This comparative analysis of Bangladesh and India demonstrates that legal responses to cybercrime are shaped not only by technological necessity but also by broader political, institutional, and constitutional contexts. The study concludes that Bangladesh's current cybercrime regime remains structurally fragile, characterized by over-criminalization, weak procedural safeguards, and limited alignment with international norms. Frequent legislative changes without substantive reform have failed to address core concerns related to legal certainty and human rights protection. Unless these structural issues are addressed, cybercrime laws in Bangladesh risk further erosion of public trust and democratic accountability. India, by contrast, illustrates how constitutional adjudication and incremental reform can contribute to a more balanced cyber legal framework. While enforcement challenges persist, particularly in relation to capacity and coordination, India's experience demonstrates the importance of judicial oversight, rights-based interpretation, and complementary regulatory instruments such as data protection law. Ultimately, the article argues that effective cybercrime governance cannot rely solely on punitive legislation. It requires a holistic approach that integrates precise legal drafting, procedural fairness, institutional capacity, international cooperation, and respect for fundamental rights. As digitalization deepens across South Asia, the experiences of Bangladesh and India offer valuable lessons for other developing jurisdictions seeking to navigate the complex terrain of cybercrime regulation.

References

1. Amnesty International. (2022). Bangladesh: Digital Security Act and the Shrinking Space for Freedom of Expression. Amnesty International Publications.
2. Amnesty International. (2024). South Asia: Cyber Laws, Surveillance and Human Rights. Amnesty International.
3. Bhandari, V. (2024). Regulating Personal Data in India: A Critical Appraisal of the Digital Personal Data Protection Act 2023. Indian Journal of Law and Technology, 20(1), 45–78.
4. Brenner, S. W. (2019). Cybercrime and the Law: Challenges, Issues, and Outcomes. Oxford University Press.
5. Clough, J. (2015). Principles of Cybercrime (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139023996.
6. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Strasbourg: Council of Europe.
7. Council of Europe. (2023). Cybercrime Legislation and Human Rights Safeguards. Council of Europe Publishing.
8. De Hert, P., & Papakonstantinou, V. (2016). The New General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review, 32(2), 179–194.https://doi.org/10.1016/j.clsr.2016.02.006.
9. Khan, M. R. (2024). Cyber security reform in Bangladesh: Legal continuity or cosmetic change? Asian Journal of Comparative Law, 19(2), 211–238. https://doi.org/10.1017/asjcl.2024.11.
10. Mendel, T. (2010). Restrictions on Freedom of Expression under International Law. UNESCO.
11. National Crime Records Bureau (NCRB). (2023). Crime in India 2022: Statistics on Cybercrime. Ministry of Home Affairs, Government of India.
12. Rahman, M. (2018). Digital Security Laws and Freedom of Expression in Bangladesh. Journal of South Asian Law, 5(1), 89–115.

13. Rahman, S., & Islam, M. T. (2021). Cyber governance and digital authoritarianism in Bangladesh. Third World Quarterly, 42(9), 2035–2052.https://doi.org/10.1080/01436597.2021.1903314
14. Singh, P. (2020). India's Cyber Law Framework: Evolution, Enforcement, and Challenges. Computer Law & Security Review, 36, 105392. https://doi.org/10.1016/j.clsr.2019.105392.
15. Svantesson, D. (2017). Solving the Internet Jurisdiction Puzzle. Oxford University Press.
16. UN Human Rights Committee. (2011). General Comment No. 34: Article 19 – Freedoms of opinion and expression. United Nations.
17. United Nations Office on Drugs and Crime (UNODC). (2021). Cybercrime and electronic evidence: Legal and practical challenges. United Nations.
18. United Nations Office on Drugs and Crime (UNODC). (2023). Global cybercrime trends and responses. United Nations.
19. Wall, D. S. (2017). Cybercrime: The transformation of crime in the information age (2nd ed.). Polity Press.
20. Wright, D., & De Hert, P. (Eds.). (2016). Privacy, data protection and cyber security in Europe. Springer. https://doi.org/10.1007/978-3-319-25361-0.
21. Zittrain, J. (2014). The future of the Internet and How to Stop It. Yale University Press.