Journal of Law and Human Rights
*Volume 5, Issuse No. 1, 2025*
**P-ISSN: 1998-4278**

# Digital Media and Cybercrime Awareness in Bangladesh: A Legal and Societal Implication

**Shahinur Rahman**
PhD Scholar, Faculty of Law, Mangalayatan University, India

**ABSTRACT**

The rapid expansion of digital media in Bangladesh has revolutionized communication, commerce, governance, and education. Yet, this transformation has also heightened vulnerabilities to cybercrime, including fraud, identity theft, hacking, cyber harassment, and misinformation campaigns. Bangladesh's legal responses through the Information and Communication Technology (ICT) Act 2006, the Digital Security Act (DSA) 2018, and the Cyber Security Act (CSA) 2023 reflect efforts to manage these threats, though each framework contains notable strengths and weaknesses. This paper explores cybercrime awareness and legal safeguards in Bangladesh, situating them within societal and technological contexts. Using a qualitative, socio-legal approach, the study identifies the causes of cybercrime, societal vulnerabilities, and gaps in enforcement. Findings demonstrate that while Bangladesh has made progress in digitization, limited cyber literacy, weak law enforcement capacity, and legal ambiguities undermine effective protection. The paper argues for comprehensive reforms, including digital literacy initiatives, institutional strengthening, and international collaboration. By situating cybercrime at the intersection of technology, law, and society, this article contributes to global scholarship on digital transformation in developing nations.

**Keywords:** Digital Media, Cybercrime, Digital Security Act, Societal Impact

## Introduction

Bangladesh has witnessed a remarkable digital transformation over the past two decades, primarily driven by the government's "Digital Bangladesh" initiative, launched in 2009. The strategy aimed to enhance access to technology, promote e-governance, expand internet penetration, and encourage innovation across economic and social sectors. As a result, the number of internet subscribers increased from fewer than 20 million in 2010 to more than 130 million by 2025 (Bangladesh Telecommunication Regulatory Commission [BTRC], 2024). This digital revolution has created unprecedented opportunities for communication, education, commerce, and civic engagement.

Social media platforms such as Facebook, YouTube, TikTok, Instagram, and WhatsApp have become central to everyday life. They not only provide spaces for entertainment and interaction but also serve as marketplaces for small businesses, tools for political communication, and gateways to financial inclusion. E-commerce services and mobile financial platforms such as bKash and Nagad have transformed how people conduct transactions, bridging gaps between urban and rural communities (Bangladesh Bank, 2024). Similarly, online learning platforms have reshaped education, while e-governance initiatives have enhanced service delivery.

Despite these benefits, Bangladesh's rapid digitalization has created serious vulnerabilities to cybercrime. As more citizens engage online, threats such as phishing, hacking, online fraud, identity theft, revenge pornography, and misinformation campaigns have escalated (Ahmed, 2022). Cyber harassment, particularly targeting women and young people, is growing at alarming rates (Haque, 2021). Government websites have been subject to hacking attempts, while businesses face increasing risks of data breaches and financial fraud (World Bank, 2024).

Recognizing these risks, the government enacted successive pieces of legislation the ICT Act 2006, the DSA 2018, and the CSA 2023 to regulate and combat cybercrime. While these laws aim to strengthen digital security, they have generated debates over enforcement effectiveness, freedom of expression, and institutional preparedness (Article 19, 2019; Freedom House, 2024).

The core objectives of this paper are threefold:

1. To explore the relationship between digital media growth and cybercrime vulnerabilities in Bangladesh.
2. To examine the legal frameworks addressing cybercrime and identify their strengths and weaknesses.
3. To analyze the societal implications of cybercrime, including economic, psychological, and political effects.

This study contributes to academic and policy debates by emphasizing the need for a multi-dimensional response combining legal reform, public awareness, institutional strengthening, and international collaboration to ensure a safe and inclusive digital ecosystem in Bangladesh.

**Conceptual Framework**

The study of cybercrime in Bangladesh requires a multi-layered conceptual approach, one that acknowledges the interplay between technology, law, and society. Cybercrime is not merely a technical or legal issue it is also a socio-political and economic phenomenon. To capture this complexity, this paper adopts a socio-legal framework that integrates the following dimensions:

**1. Technological Dimension**

Cybercrime thrives on digital infrastructures such as the internet, social media platforms, mobile applications, and online banking systems. Weak security protocols, outdated systems, and poor digital hygiene make these infrastructures vulnerable. Understanding the technical aspects such as phishing methods, malware, and data breaches is essential for designing preventive mechanisms (UNODC, 2021).

**2. Legal Dimension**

The presence of laws such as the ICT Act (2006), DSA (2018), and CSA (2023) indicates Bangladesh's recognition of cybercrime threats. However, the efficacy of these laws depends on clarity of provisions, enforcement capacity, and their alignment with international standards. The legal framework also interacts with fundamental rights, such as freedom of expression and privacy (Article 19, 2019).

**3. Societal Dimension**
The social impact of cybercrime ranging from online harassment and misinformation to economic fraud underscores the role of digital literacy, cultural attitudes, and citizen awareness. For example, patriarchal norms amplify gendered cyber violence, while political polarization magnifies disinformation campaigns (Haque, 2021).

**4. Institutional Dimension**
Effective enforcement requires capable institutions such as the Cyber Tribunal, BGD e-Gov CIRT, and cybercrime units within law enforcement. However, these institutions often suffer from underfunding, limited training, and inadequate digital forensics resources (ICNL, 2024).

This socio-legal model recognizes cybercrime as the outcome of both structural vulnerabilities (in technology and institutions) and behavioral factors (in citizen use of digital media). Figure 1 (not included here but suggested for a journal version) would depict this framework, showing how digital media growth leads to cyber risks, which interact with legal responses and societal impacts.

**Digital Media in Bangladesh**

**1. Expansion of Internet and Social Media**
Bangladesh has experienced a dramatic rise in internet penetration, from less than 15% of the population in 2010 to nearly 80% in 2025 (BTRC, 2024). Mobile internet, facilitated by affordable smartphones, accounts for the majority of this growth. Social media has become an essential aspect of daily life, with over 130 million active users engaging in Facebook, YouTube, TikTok, and other platforms. These platforms are not only entertainment hubs but also critical tools for commerce, education, and political mobilization.

**2. E-Commerce and Digital Finance**
The rise of e-commerce platforms such as Daraz, Evaly, and AjkerDeal has reshaped consumer behavior, enabling home delivery, digital marketplaces, and cross-border trade. Simultaneously, mobile financial services (MFS) like bKash, Rocket, and Nagad have revolutionized financial inclusion. According to Bangladesh Bank (2024), more than 120 million MFS accounts are active, processing billions in daily transactions. However, this digital revolution has been accompanied by a surge in online fraud, SIM swap scams, and fake payment links, posing serious cybercrime risks.

**3. Digital Media in Education and Governance**
The COVID-19 pandemic accelerated the adoption of digital platforms for education, with universities and schools relying heavily on Zoom, Google Classroom, and locally developed apps. Similarly, the government has introduced e-governance services, including online tax filing, birth registration, and land record management. These initiatives improve efficiency but also expose state databases to cyberattacks.

**4. Challenges of Rapid Digitalization**
The rapid growth of digital media has outpaced the development of cybersecurity infrastructure. Many citizens lack basic cyber literacy, such as identifying phishing links or enabling two-factor authentication. Additionally, the absence of robust data protection laws exacerbates risks of personal data misuse. In rural areas, low awareness makes citizens particularly vulnerable to online scams, while urban populations face more sophisticated cyber threats like ransomware and hacking (World Bank, 2024).

**5. Opportunities and Risks**
Digital media in Bangladesh provides opportunities for innovation, entrepreneurship, and global connectivity. However, its risks include:

- Misinformation campaigns influencing politics and elections.
- Online harassment, especially targeting women, journalists, and activists.
- Financial fraud, undermining trust in MFS and e-commerce.
- Cross-border cybercrime, exploiting weak international cooperation.

Thus, while digital media is a powerful engine of modernization, its unchecked expansion without adequate safeguards amplifies the threat landscape.

**Causes of Cybercrime**
Cybercrime in Bangladesh arises from a combination of structural, economic, social, and technological factors. These causes are multi-dimensional and interact with one another, creating a complex ecosystem of vulnerabilities.

**1. Economic Motivations**
Bangladesh faces persistent challenges of unemployment and underemployment, particularly among youth. Many individuals view cybercrime as a lucrative alternative in the absence of stable income opportunities. Fraudulent activities such as mobile banking scams, phishing schemes, and ATM card skimming have become common. For example, mobile financial services report thousands of fraud cases every month, ranging from fake cash-out requests to manipulated SMS notifications (Bangladesh Bank, 2024).

**2. Technological Illiteracy**
Despite high internet penetration, a majority of users lack basic cybersecurity knowledge. Weak password practices, inability to detect phishing emails, and ignorance of privacy settings make individuals easy targets. According to Rouf (2024), more than 60% of rural internet users in Bangladesh cannot differentiate between authentic and fake digital content.

**3.Weak Cyber security Infrastructure**
Both government and private institutions suffer from inadequate investment in cybersecurity. Banks and financial institutions often fail to implement advanced firewalls or encryption systems, leading to data leaks. In 2022, several Bangladeshi government websites were hacked by international hacker groups, exposing sensitive public records (ICNL, 2024).

**4. Social and Cultural Factors**
Bangladesh's patriarchal society amplifies certain forms of cybercrime, particularly gender-based violence online. Women often face harassment, blackmail through leaked personal photos, and cyberstalking. The misuse of social media for spreading fake news, political propaganda, and communal hate speech also fuels cyber incidents (Haque, 2021).

**5. Law Enforcement Challenges**
The capacity of law enforcement agencies remains limited. Digital forensic labs are underdeveloped, and police officers often lack specialized training in cyber investigations. As a result, the conviction rate in cybercrime cases is low. Victims frequently report dissatisfaction due to delays and lack of follow-up in investigations (Ahmed, 2022).

**6. International Dimensions of Cybercrime**
A significant share of cybercrimes targeting Bangladesh originate from outside its borders. Phishing attacks, online gambling networks, and ransomware schemes often involve perpetrators from other countries. Weak international cooperation mechanisms make it difficult to prosecute cross-border offenders (UNODC, 2020).

**Cybercrime Laws in Bangladesh**
Bangladesh has enacted a series of laws to address the rising tide of cybercrime. These laws reflect both progress and controversy, as policymakers struggle to balance security with rights to privacy and freedom of expression.

**1. ICT Act 2006**
The Information and Communication Technology (ICT) Act 2006 was the first major attempt to criminalize digital offenses. Key provisions included:

- Penalizing hacking, identity theft, and unauthorized access to digital systems.
- Criminalizing electronic forgery and online fraud.
- Establishing guidelines for electronic evidence.

Controversy: Section 57 of the ICT Act became notorious for its vague wording, criminalizing "publishing fake, obscene, or defamatory information in electronic form." This provision was widely criticized for being used to suppress dissent, journalists, and activists. Following sustained criticism, Section 57 was repealed and replaced by the Digital Security Act (DSA) 2018 (Article 19, 2019).

**2. Digital Security Act 2018 (DSA)**
The DSA 2018 sought to modernize Bangladesh's cybercrime laws by addressing a broader range of offenses, including:

- Cyber terrorism and digital propaganda.
- Unauthorized access to government databases.
- Online defamation and harassment.
- Misuse of biometric data.

The Act also created the Digital Security Agency and authorized the establishment of specialized cybercrime tribunals.

Criticism: Despite these advancements, the DSA has been criticized for being overly restrictive of free speech. International watchdogs argue that the law has been misused to silence political opposition and journalists (Freedom House, 2024).

**3. Cyber Security Act 2023 (CSA)**
The CSA 2023 was introduced to replace and harmonize the ICT Act and DSA, with the intention of aligning cybercrime laws with international.

**Weaknesses of the Laws**

Despite legislative progress, several weaknesses persist:

1. **Ambiguity in Legal Definitions:** Terms such as "digital security threat" or "cyber harassment" are vaguely defined, creating scope for arbitrary enforcement (Article 19, 2019).
2. **Freedom of Expression Concerns:** DSA and CSA provisions may criminalize legitimate online speech, resulting in self-censorship (Freedom House, 2024).
3. **Enforcement Capacity:** Limited expertise in digital forensics and investigation impedes law enforcement effectiveness (ICNL, 2024).
4. **Public Awareness Gap:** Citizens often lack knowledge of reporting mechanisms and cybersecurity best practices (Rouf, 2024).
5. **International Coordination:** Weak collaboration with foreign agencies reduces the ability to prosecute cross-border cybercrime (UNODC, 2021).

**Societal Effects of Cybercrime**

Cybercrime impacts multiple dimensions of Bangladeshi society:

- **Economic Impact:** Financial fraud undermines trust in digital banking and mobile financial services (Bangladesh Bank, 2024).
- **Psychological and Social Impact:** Cyber harassment and revenge pornography cause trauma, especially among women and youth (Haque, 2021).
- **Political Impact:** Misinformation campaigns affect election integrity and public trust in institutions (Freedom House, 2024).
- **E-Governance Impact:** Hacking government websites erodes citizen confidence in digital services (World Bank, 2024).
- **Digital Divide:** Vulnerable populations face greater exposure due to lack of digital literacy (Rouf, 2024).

**Findings**

This study identifies several key findings on the intersection of digital media, cybercrime, law, and society in Bangladesh:

**1. Rapid digitalization has outpaced security frameworks**

With nearly 80% internet penetration (BTRC, 2024), Bangladesh has undergone a dramatic digital transformation. However, cybersecurity infrastructure, public awareness, and institutional readiness remain inadequate.

**2. Cybercrime is driven by socio-economic and technological vulnerabilities**

High youth unemployment, poor cyber literacy, and weak institutional safeguards contribute to the rise in cyber offenses.

**3. Legal frameworks exist but suffer from overreach and weak enforcement**

Laws like the ICT Act (2006), DSA (2018), and CSA (2023) criminalize a wide range of offenses but are criticized for vague language and misuse against journalists and civil society (Article 19, 2019; Freedom House, 2024).

**4. Institutional limitations undermine deterrence**

Cyber tribunals, police cyber units, and digital forensics labs lack sufficient resources, leading to delays and low conviction rates (Ahmed, 2022).

**5. Societal consequences are severe and multifaceted**
Cybercrime erodes trust in digital finance, damages mental health, fuels political polarization, and discourages women's participation in online platforms (Haque, 2021).

**6. International dimensions are neglected**
Many cybercrimes involve cross-border actors, yet Bangladesh lacks robust treaties or regional frameworks for cooperation (UNODC, 2021).

**Recommendations**
Based on the findings, the following recommendations are proposed:

**1. Strengthening Digital Literacy**
Launch nationwide digital literacy campaigns through schools, universities, and community centers. Integrate cybersecurity education into curricula, emphasizing password security, phishing awareness, and responsible online behavior.

**2. Enhancing Law Enforcement Capacity**
Establish specialized cybercrime units in every district police station. Provide advanced digital forensics training and invest in forensic labs. Encourage collaboration between police, telecom companies, and financial institutions.

**3. Legal Reform and Safeguards**
Revise vague provisions in the CSA 2023 to align with international human rights standards. Ensure a balance between national security and freedom of expression by introducing judicial oversight for online content takedowns.

**4. Institutional Strengthening**
Increase funding for Cyber Tribunals to reduce case backlogs. Expand the capacity of BGD e-Gov CIRT to cover not only government but also private sector digital infrastructure.

**5. International Collaboration**
Develop bilateral and multilateral agreements with regional partners (e.g., SAARC countries) for cross-border cybercrime investigation. Join global initiatives such as the Budapest Convention on Cybercrime for standardized international cooperation.

**6. Gender-Sensitive Interventions**
Establish women-focused cyber helplines and safe reporting channels. Train law enforcement on gender-sensitive approaches to handle cases of online harassment and cyber violence.

**7. Public-Private Partnerships**
Partner with telecom operators, banks, and e-commerce platforms to develop early-warning systems for fraud. Promote corporate investment in cybersecurity infrastructure and staff training.

**Conclusion**
Digital media has revolutionized Bangladesh's social, economic, and political landscapes, yet it has also exposed citizens to unprecedented cyber risks. The country's legal response—through the ICT Act (2006), DSA (2018), and CSA (2023)—shows commendable recognition of the threat but suffers from vague provisions, weak enforcement, and overreach into civil liberties.

Cybercrime in Bangladesh is not merely a legal problem; it is a societal challenge. It affects financial security, women's rights, mental health, democratic participation, and trust in state institutions. Addressing it requires a holistic approach that combines law reform, institutional strengthening, citizen awareness, and international collaboration.

If Bangladesh is to realize the vision of "Digital Bangladesh" while safeguarding its citizens, it must adopt policies that balance innovation with protection, security with rights, and modernization with justice. Only then can digital media serve as a true engine of inclusive progress.

**References**


1. Ahmed, S. (2022). Cybercrime in Bangladesh: Challenges and prospects of legal framework. Dhaka University Law Journal, 33(2), 45–67.
2. Ahmed, T., &Rahman, M. (2021).Social media, cyberbullying, and youth mental health in Bangladesh. Asian Journal of Social Sciences and Humanities, 10(4), 112–126.
3. Akhter, F., & Sultana, S. (2020). Gendered dimensions of cyber harassment in Bangladesh: Policy gaps and recommendations. Journal of Gender Studies, 29(6), 745–760.
4. Article 19. (2019). Bangladesh: Analysis of the Digital Security Act 2018. Article 19. https://www.article19.org
5. Bangladesh Bank. (2024). Annual report on mobile financial services fraud and digital transactions. Bangladesh Bank.
6. Bangladesh Telecommunication Regulatory Commission (BTRC).(2024). Internet and mobile penetration statistics in Bangladesh.BTRC.
7. Chowdhury, M. A. (2021). Cybersecurity threats and financial fraud in Bangladesh's banking sector. Journal of Financial Crime, 28(3), 887–902.
8. Freedom House. (2024). Freedom on the net 2024: Bangladesh. Freedom House. https://freedomhouse.org
9. Gomes, A., &Hasan, N. (2022). ICT infrastructure and cybercrime in developing countries: Evidence from Bangladesh. Journal of Information Security and Applications, 64, 103061.
10. Haque, S. (2021). Cyber violence against women in Bangladesh: Emerging issues and policy implications. International Journal of Cyber Criminology, 15(2), 256–273.
11. Hossain, A., & Karim, R. (2020). Legal responses to cybercrime in Bangladesh: An analysis of the Digital Security Act. Asian Journal of Comparative Law, 15(1), 89–105.
12. International Center for Not-for-Profit Law (ICNL).(2024). Cybercrime legislation and civic space in Bangladesh.ICNL. https://www.icnl.org
13. Islam, M. T. (2021). Digital governance and cyber resilience in Bangladesh. Journal of Public Administration and Policy Research, 13(3), 44–57.
14. Khan, S., &Jahan, T. (2020). Mobile banking fraud in Bangladesh: Risks, responses, and resilience. South Asian Journal of Business and Management Cases, 9(2), 167–179.
15. Mamun, M. A. (2023). Online disinformation and electoral integrity in Bangladesh. Asian Politics & Policy, 15(2), 335–350.
16. Rahman, M., &Rouf, K. (2022).Digital divide, cybercrime, and social inequality in Bangladesh. Information Development, 38(4), 573–585.
17. Rouf, K. (2024). Cybersecurity literacy and community awareness in Bangladesh: An empirical study. BRAC Institute of Governance and Development.
18. Sarker, M. (2023). Enforcement challenges of cybercrime laws in Bangladesh: The case of CSA 2023. Bangladesh Journal of Criminology, 4(1), 21–40.

19. Transparency International Bangladesh (TIB).(2022). Digital governance and corruption risks in Bangladesh.TIB.
20. UNDP. (2022). E-governance and digital security in South Asia: Bangladesh country profile. United Nations Development Programme.
21. United Nations Office on Drugs and Crime (UNODC).(2021). Global report on cybercrime and international cooperation.UNODC.
22. World Bank. (2024). Digital governance readiness assessment: Bangladesh 2024. The World Bank.
23. Zaman, H., & Alam, S. (2021). Data privacy and protection laws in Bangladesh: A critical review. Computer Law & Security Review, 41, 105556.