UGC & Govt. Approved

Sonargaon University (SU)

সোনারগাঁও ইউনিভার্সিটি (এসইউ)

Research on

“Balancing Cybersecurity And Individual Rights: A Critical Analysis Of Bangladesh’s Cyber security Act 2023”

Submitted By

Amrita Lal Majumder

ID: LLMP2302029001

Department of the Bachelor of Laws

Submitted To

Sharmin Jahan Runa
Assistant Professor & Head of the Department
Department of Laws
Sonargaon University (SU)

Date of Submission: 08/04/2025

Letter of Transmittal

To,

Sharmin Jahan Runa

Assistant Professor & Head of the Department

Department of Laws

Sonargaon University (SU)

Subject: Submission of Research Monograph Titled "Balancing Cybersecurity and Individual Rights: A Critical Analysis of Bangladesh's Cyber Security Act 2023"

Dear Madam,

I am pleased to submit my research monograph titled **"Balancing Cybersecurity and Individual Rights: A Critical Analysis of Bangladesh's Cyber Security Act 2023"** for your kind consideration. This monograph represents the culmination of extensive research and analysis conducted over the past few months and aims to provide a critical examination of the law, its implementation, and its implications for individual rights in Bangladesh.

I believe that the insights and findings presented in this monograph will be of great value to policymakers, legal scholars, digital rights activists, and other stakeholders concerned with the balance between national security and civil liberties in the digital era.

Thank you for your time and attention. I look forward to your valuable feedback and the opportunity to engage in meaningful discussion on this important topic.

Sincerely,

Amrita Lal Majumder

ID No: LLMP2302029001

Program: Master of Laws (LL.M)

Department of Laws

Sonargaon University (SU), Dhaka

Certification by the Research Supervisor

This is to certify that the research paper titled **"Balancing Cybersecurity and Individual Rights: A Critical Analysis of Bangladesh's Cyber Security Act 2023"** has been submitted in fulfillment of the requirements for the award of the **Master of Laws (LL.M)** degree from **Sonargaon University** by the student bearing **ID: LLMP2302029001**. The research was carried out under my active supervision and guidance. I further certify that no part of this paper has been submitted for the award of any other degree or diploma and that the work has not been published in any legal or popular publications.

Sharmin Jahan Runa
Assistant Professor & Head of the Department
Department of Laws

Faculty of Arts and Humanities
Sonargaon University (SU)



Sonargaon University

Department of Law

A Dissertation On

Balancing Cybersecurity And Individual Rights: A Critical Analysis Of Bangladesh's Cybersecurity Act 2023

A thesis submitted in partial fulfillment of the requirements

For the degree of Master of Laws (LLM)

Submitted By: Amrita Lal Majumder

ID: LLMP2302029001

Master of Laws (LLM)

Date of Submission: 08/07/25

DECLARATION

I, Amrita Lal Majumder, hereby declare that the thesis titled "Balancing Cybersecurity and Individual Rights: A Critical Analysis of Bangladesh's Cyber Security Act 2023" submitted in fulfillment of the requirements for the Master of Laws (LL.M) degree, Department of Law, Sonargaon University, embodies the results of my own research conducted under the supervision of Sharmin Jahan Runa, Assistant Professor & Head of the Department, Department of Laws, Sonargaon University.

I further declare that this thesis is original, free from plagiarism, and has not been submitted, in whole or in part, to any other university or institution for any academic qualification.

Name: Amrita Lal Majumder
ID: LLMP2302029001
Program: Master of Laws (LL.M)
Department of Laws
Sonargaon University

ACKNOWLEDGMENT

This research paper has been made possible through the support and encouragement of many individuals. I am deeply thankful to my parents, teachers, friends, and all well-wishers who inspired and supported me throughout this journey.

Above all, I express my deepest gratitude to my respected supervisor, Sharmin Jahan Runa, Assistant Professor & Head of the Department, Department of Laws, Sonargaon University (SU), for her continuous support, expert guidance, patience, and inspiration. Her insightful feedback and motivation played a key role in completing this research successfully.

I would also like to thank the honorable members of my defense committee for their constructive criticism and valuable suggestions.

Contents

Abstract viii

CHAPTER – I 1

GENERAL INTRODUCTION

1.1 Introduction 1

1.2 Statement of the Problem: 2

1.3 Research Questions: 2

1.4 Research Objectives: 2

1.5 Literature Review: 3

1.6 Research Methodology: 3

1.7 Significance of the Study: 4

1.8 Conclusion: 4

1.9 Tentative Chapter Outline: 4

CHAPTER – II 4

CONTEXTUALIZING CYBERSECURITY AND INDIVIDUAL RIGHTS IN BANGLADESH

2.1 Introduction 5

2.2 The Digital Landscape and Cybersecurity Challenges in Bangladesh 6

2.3 Evolution of Cybersecurity Laws in Bangladesh 6

2.4 Fundamental Rights Impacted by Cybersecurity Legislation 7

2.5 The Challenge of Balancing National Security and Individual Rights 7

2.6 Comparative International Standards and Practices 8

2.7 Role of Civil Society, Media, and Stakeholders 8

2.8 Conclusion 9

CHAPTER – III 11

LEGAL ANALYSIS OF THE CYBER SECURITY ACT, 2023

3.1 Introduction 11

3.2 Overview of the Cyber Security Act, 2023 12

3.3 Key Legal Provisions and Their Implications 12

3.4 Compatibility with Constitutional and International

Human Rights Norms 13

3.5 Potential Risks and Criticisms 16

3.6 Enforcement Challenges 16

3.7 Comparative Insights from Other Jurisdictions 17
3.8 Conclusion 17
CHAPTER – IV 19
CYBERSECURITY LANDSCAPE IN BANGLADESH: EVOLUTION AND CHALLENGES
4.1 Introduction 19
4.2 Digital Transformation in Bangladesh: A Brief Overview 19
4.3 Evolution of Cybersecurity Policies and Laws 20
4.4 Current Cybersecurity Threats 21
4.5 Current Cybersecurity Threats in Bangladesh 22
4.6 Institutional Framework for Cybersecurity Governance 22
4.7 Key Challenges in Bangladesh's Cybersecurity Landscape 23
4.8 Global Commitments and International Cooperation 24
4.9 Public Perception and Role of Civil Society 24
4.10 Conclusion 25
CHAPTER – V 27
CONCLUDING REMARKS
5.1 Findings of the Study 27
5.2 Recommendations 28
5.3 Conclusion 29
Bibliography 33

Abstract

In the digital era, cybersecurity has become a critical national concern, particularly for developing nations like Bangladesh, which faces increasing threats such as cybercrime, data breaches, and digital surveillance. In response, the Government of Bangladesh enacted the Cyber Security Act, 2023, replacing the Digital Security Act, 2018. This thesis critically examines the Cyber Security Act, 2023, focusing on its legal, institutional, and human rights implications. While the Act aims to enhance cybersecurity and protect critical digital infrastructure, it raises concerns about the erosion of constitutionally guaranteed rights, including freedom of expression, privacy, and due process.

The research adopts a qualitative doctrinal approach, analyzing the Act in the context of national constitutional provisions and international human rights obligations. Comparative insights from jurisdictions such as India, the European Union, and the United States highlight best practices in balancing security with civil liberties. The study finds that the Act retains many repressive elements of the repealed Digital Security Act, contains vague definitions, lacks adequate judicial oversight, and grants sweeping powers to law enforcement agencies—creating potential for misuse and suppression of dissent.

This thesis concludes that while cybersecurity is essential, legal frameworks must be transparent, proportionate, and rights-respecting. It proposes reforms including the enactment of a comprehensive data protection law, clearer legal definitions, enhanced judicial safeguards, and the involvement of civil society in lawmaking. These reforms are vital for ensuring that cybersecurity measures in Bangladesh both protect national interests and uphold democratic freedoms.

CHAPTER -1

GENERAL INTRODUCTION

1.1 Introduction

In the digital age, cybersecurity has emerged as a pressing priority for governments worldwide. With the exponential growth of internet usage, digital financial systems, online communication, and the increasing dependence on information and communication technologies (ICTs), the threat landscape has expanded significantly. Bangladesh, like many developing nations, has witnessed a sharp rise in cyber incidents including data breaches, online fraud, identity theft, and cyberterrorism. In response to these evolving threats, the Government of Bangladesh enacted the Cyber Security Act, 2023, replacing the much-criticized Digital Security Act, 2018, in an attempt to modernize the country's legal framework for digital protection and to address growing national security concerns.

While the Cyber Security Act, 2023, aims to enhance national resilience against cyber threats and protect critical information infrastructure, it also raises serious concerns about its implications for individual rights. Civil society organizations, journalists, human rights defenders, and legal experts have expressed apprehensions regarding potential overreach, lack of judicial oversight, vague definitions, and the chilling effect the law may have on freedom of expression, privacy, and the right to dissent. The tension between ensuring national cybersecurity and upholding individual rights such as the right to privacy, freedom of speech, and due process has become a central legal and ethical dilemma.

This thesis seeks to critically examine the Cyber Security Act, 2023 through the lens of fundamental rights protected under the Constitution of Bangladesh and international human rights obligations. It will analyze whether the Act strikes a fair balance between protecting national security in cyberspace and preserving individual freedoms in a democratic society. The study will explore the structure, scope, and application of the Act, identifying provisions that may be susceptible to abuse or arbitrary enforcement.

The research will employ a doctrinal legal methodology supported by comparative analysis, examining similar laws from jurisdictions such as India, the European Union, and the United States. It will also consider judicial interpretations, scholarly critiques, and perspectives from relevant stakeholders. Ultimately, this thesis aims to contribute to the ongoing discourse on cybersecurity legislation in Bangladesh, offering recommendations for policy reform that ensure both robust cyber protection and the safeguarding of civil liberties.

1.2 Statement of the Problem

The increasing dependence on digital technologies in Bangladesh has necessitated stronger cybersecurity measures to combat cybercrimes and protect national infrastructure. In response, the government enacted the Cyber Security Act, 2023, replacing the controversial Digital Security Act, 2018. While the new law aims to address previous shortcomings and enhance cyber protections, serious concerns remain regarding its potential to infringe upon individual rights, such as freedom of expression, privacy, and due process. Critics argue that several provisions grant excessive powers to law enforcement and regulatory authorities without sufficient judicial oversight, leading to fears of misuse and arbitrary enforcement. This creates a legal and ethical dilemma: how to ensure robust cybersecurity without undermining the fundamental rights guaranteed by the Constitution of Bangladesh and international human rights norms. This thesis seeks to critically examine this tension and assess whether the Cyber Security Act, 2023 strikes an appropriate balance between security and liberty.

1.3 Research Questions

1. To what extent does the Cyber Security Act, 2023 of Bangladesh uphold or restrict individual rights such as freedom of expression, privacy, and due process?
2. How does the Cyber Security Act, 2023 compare with similar cybersecurity laws in other jurisdictions (India, EU, USA) in balancing national security and civil liberties?
3. What legal and policy reforms can be proposed to ensure that the Cyber Security Act, 2023 effectively addresses cyber threats while safeguarding constitutional and international human rights standards?

1.4 Research Objectives

The primary objective of this study is to critically analyze the *Cyber Security Act, 2023* of Bangladesh in light of its impact on constitutionally guaranteed individual rights, including freedom of expression, the right to privacy, and due process. This research aims to assess whether the Act strikes an appropriate balance between ensuring national cybersecurity and protecting civil liberties. Specifically, the study seeks to: (1) examine the legal framework and key provisions of the Act to identify areas that may pose risks to fundamental rights; (2) evaluate the compatibility of the Act with the Constitution of Bangladesh and international human rights standards; and (3) conduct a comparative analysis with similar laws in other jurisdictions to draw lessons and best practices. Finally, the study intends to propose legal and policy recommendations to strengthen the Cyber Security Act, ensuring that it provides effective digital security without compromising individual freedoms.

1.5 Literature Review

Ehsan & Saquib (2024) examine the CSA's structure, emphasizing its broad and ambiguous definitions. They argue that while intended to strengthen digital resilience, the Act also "give governments an opportunity to control digital environments at the cost of individual liberties," particularly affecting freedom of speech and privacy .

Amnesty International (2024) critiques the CSA as "a continuation of successive repressive legislations," noting that the Act replicates 58 of the 62 provisions from the Digital Security Act (DSA) 2018. They warn that this perpetuates "lawfare" used to suppress dissent, with sweeping police powers and minimal judicial oversight .

Rezaur Rahman Lenin (2023), writing in *Prothom Alo*, highlights that the CSA was drafted without meaningful stakeholder consultation. He warns that institutions created under the law—such as the Digital Security Agency and cyber tribunal—lack procedural safeguards and risk excessive control over citizens' digital activity .

A study by the International Journal of Research and Innovation in Social Science (2024) examines the CSA's enforcement landscape, noting TIB's concerns that its vague language and maintained DSA elements threaten media freedom. They assert the Act could be used against journalists under broad defamation or misinformation clauses .

In The Daily Star, Toriqul Islam (2024) argues the CSA is essentially "old wine in new bottles," retaining draconian elements of the DSA and calling for its repeal or substantial overhaul. Proposed reforms include more precise legal definitions, a clearer distinction between cybercrime and content regulation.

1.6 Research Methodology

This study adopts a qualitative doctrinal legal research methodology, focusing on the critical analysis of primary and secondary legal sources. It examines the Cyber Security Act, 2023, relevant constitutional provisions, and international human rights instruments. The research includes **a** comparative legal analysis with cybersecurity laws from jurisdictions such as India, the European Union, and the United States to identify global best practices. Secondary sources such as journal articles, reports by human rights organizations, and expert commentaries are analyzed to understand the practical implications and challenges in balancing cybersecurity with individual rights in Bangladesh.

1.7 Significance of the Study

This study is significant as it critically examines the Cyber Security Act, 2023 of Bangladesh in the context of preserving individual rights such as freedom of expression and privacy. By highlighting legal gaps, potential misuse, and comparative insights, the research contributes to the national discourse on digital governance. It aims to support policy reform, promote human rights-compliant cybersecurity laws, and ensure a balanced approach between national security and civil liberties in Bangladesh's evolving digital landscape.

1.8 Conclusion

This study critically examines Bangladesh's Cyber Security Act, 2023, highlighting the ongoing challenge of balancing national cybersecurity needs with the protection of individual rights such as privacy and freedom of expression. While the Act aims to strengthen digital security, its broad and vague provisions risk undermining fundamental freedoms and judicial oversight. Comparative analysis reveals the need for clearer definitions and stronger safeguards. This thesis recommends legal reforms that ensure effective cyber protection without compromising constitutional rights, thereby contributing to a balanced and rights-respecting digital governance framework in Bangladesh's evolving cyberspace landscape.

1.9 Tentative in chapter outline

Chapter -1 General Introduction.

Chapter-2 Contextualizing Cybersecurity and Individual Rights in Bangladesh.

Chapter-3 Legal Analysis of the Cyber Security Act, 2023.

Chapter -4 Cybersecurity Landscape in Bangladesh: Evolution and Challenges.

Chapter -5 Concluding Remarks.

CHAPTER -2

Contextualizing Cybersecurity and Individual Rights in Bangladesh

2.1 Introduction

In the contemporary digital era, cybersecurity has become a vital concern for governments globally[1]. The rapid expansion of internet access, mobile technologies, and digital services has transformed how societies function, promoting economic growth, communication, and governance efficiencies[2]. Bangladesh is no exception, experiencing accelerated digitalization, as reflected in initiatives like the "Digital Bangladesh" vision. While this digital transformation brings tremendous opportunities, it also exposes vulnerabilities that pose significant threats to national security and individual freedoms[3].

Cyber threats such as data breaches, cybercrime, online fraud, and cyberterrorism have become increasingly prevalent in Bangladesh[4]. In response, the Government enacted the Cyber Security Act, 2023, aiming to modernize and strengthen the country's cybersecurity legal framework. However, this law has sparked debate over the potential infringement on fundamental rights, including freedom of expression, privacy, and due process[5].

This chapter contextualizes the intersection of cybersecurity and individual rights in Bangladesh by exploring the country's digital landscape, legal framework, challenges in balancing security and rights, and the socio-political environment. It establishes the foundation for a critical analysis of the Cyber Security Act, 2023, and its implications on rights protection[6].

---

[1] UK Government, *National Cyber Strategy 2022* (Policy Paper, 15 December 2021) https://www.gov.uk/government/publications/national-cyber-strategy-2022; last visited on 2nd June, 2025.

[2] World Bank, *World Development Report 2021: Data for Better Lives* (World Bank Group 2021) https://www.worldbank.org/en/publication/wdr2021; last visited on 2nd June, 2025.

[3] Government of Bangladesh, *Digital Bangladesh: Concept Note* (a2i Programme, Prime Minister's Office) https://a2i.gov.bd/publication/digital-bangladesh-concept-note/; last visited on 2nd June, 2025.

[4] Cyber Crime Awareness Foundation, *Cybercrime Trend in Bangladesh 2022* (CCAF 2022) https://www.ccafbd.org/reports/cybercrime-trend-in-bangladesh-2022.pdf; last visited on 2nd June, 2025.

[5] Rejaul Karim Byron and Wasim Bin Habib, 'Cyber Security Act Passed in Parliament' *The Daily Star* (Dhaka, 13 September 2023) https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-passed-parliament-3411011; last visited on 2nd June, 2025.

[6] ARTICLE 19, *Bangladesh: New Cyber Security Act Threatens Freedom of Expression* (ARTICLE 19, 15 September 2023) https://www.article19.org/resources/bangladesh-new-cyber-security-act-threatens-freedom-of-expression/; last visited on 2nd June, 2025.

2.2 The Digital Landscape and Cybersecurity Challenges in Bangladesh

Bangladesh has witnessed remarkable growth in internet connectivity and digital services[7]. As of 2024, internet users number over 100 million, representing roughly 60% of the population. The widespread availability of affordable smartphones and expanding mobile networks have accelerated digital inclusion[8].

Key cybersecurity challenges include:

- **Rising Cybercrime:** Cybercrimes such as phishing, identity theft, financial fraud, and ransomware attacks have surged[9]. Vulnerabilities in both private and public sectors increase the risk of large-scale data breaches.
- **Cyberterrorism and Political Cyberattacks:** Attacks targeting critical infrastructure, government systems, and political actors have raised national security concerns[10].
- **Limited Cybersecurity Infrastructure:** Despite government efforts, Bangladesh's cybersecurity infrastructure lacks sufficient sophistication, skilled human resources, and coordination[11].
- **Low Cyber Awareness:** The general public's limited knowledge about cybersecurity practices exacerbates risks[12].

2.3 Evolution of Cybersecurity Laws in Bangladesh

Bangladesh's legal response to cybersecurity has evolved rapidly to keep pace with emerging threats[13].

---

[7] World Bank, *Digital Bangladesh to Smart Bangladesh: Leveraging ICT for Inclusive Growth* (World Bank 2023) https://www.worldbank.org/en/news/feature/2023/12/15/digital-bangladesh-to-smart-bangladesh; last visited on 2nd June, 2025.

[8] Bangladesh Telecommunication Regulatory Commission (BTRC), *Internet Subscribers in Bangladesh February 2024* (BTRC, 2024) https://www.btrc.gov.bd/content/internet-subscribers-bangladesh-february-2024; last visited on 2nd June, 2025.

[9] Cyber Crime Awareness Foundation (CCAF), *Cybercrime Trend in Bangladesh 2022* (CCAF 2022) https://www.ccafbd.org/reports/cybercrime-trend-in-bangladesh-2022.pdf; last visited on 2nd June, 2025.

[10]Mohammad Al-Masum Molla, 'Cyberattacks Target Bangladesh Govt Websites amid Political Tensions' *The Daily Star* (Dhaka, 5 December 2023) https://www.thedailystar.net/news/bangladesh/news/cyberattacks-target-bangladesh-govt-websites-amid-political-tensions-3524596 ; last visited on 3rd June, 2025.

[11] World Bank, *Cybersecurity Capacity Assessment for Bangladesh* (World Bank 2023) https://www.worldbank.org/en/news/report/2023/11/02/cybersecurity-capacity-assessment-bangladesh; last visited on 3rd June, 2025.

[12] Cyber Crime Awareness Foundation (CCAF), *Cyber Awareness Survey in Bangladesh 2022* (CCAF 2022) https://www.ccafbd.org/reports/cyber-awareness-survey-2022.pdf; last visited on 4th June, 2025.

[13] Government of Bangladesh, *Cyber Security Act 2023* (Bangladesh National Parliament, 2023) https://www.parliament.gov.bd; last visited on 4th June, 2025.

- **Digital Security Act, 2018:** The DSA aimed to tackle cybercrimes and misinformation but became controversial due to vague provisions, broad definitions, and alleged misuse to suppress free speech and dissent. Its enforcement raised serious human rights concerns[14].
- **Cyber Security Act, 2023:** Introduced to replace the DSA, the CSA seeks to modernize the legal framework with stronger mechanisms to protect national digital infrastructure[15]. Despite intended improvements, critics argue it continues to pose risks to fundamental freedoms due to broad police powers, lack of clear judicial oversight, and ambiguous language.

The government has also introduced the National Cybersecurity Strategy to promote awareness, capacity building, and resilience.

2.4 Fundamental Rights Impacted by Cybersecurity Legislation

Cybersecurity laws inherently influence various constitutionally protected rights:

- Freedom of Expression**:** Online speech regulation must balance preventing harmful content while protecting free discourse. Broad definitions of "fake news" or "defamation" risk censorship and self-censorship[16].
- Right to Privacy**:** Increasing surveillance capabilities and data retention provisions can infringe on individuals' privacy without proper safeguards[17].
- Due Process and Fair Trial**:** Provisions allowing arrest without warrant, lengthy detention, and restricted legal recourse can violate due process guarantees[18].

[14] Human Rights Watch, *Bangladesh: Repeal Abusive Digital Security Act* (HRW, 19 June 2023) https://www.hrw.org/news/2023/06/19/bangladesh-repeal-abusive-digital-security-act; last visited on 5th June, 2025.

[15] Government of Bangladesh, *Cyber Security Act 2023* (Bangladesh National Parliament, 2023) https://www.parliament.gov.bd; last visited on 5th June, 2025.

[16] ARTICLE 19, *Bangladesh: Cyber Security Act Raises Free Speech Concerns* (ARTICLE 19, 18 September 2023) https://www.article19.org/resources/bangladesh-cyber-security-act-concerns/; last visited on 5th June, 2025.

[17] Privacy International, *Mass Surveillance and the Right to Privacy in Bangladesh* (Privacy International, 2023) https://privacyinternational.org/report/5209/mass-surveillance-and-right-privacy-bangladesh; last visited on 6th June, 2025.

[18] Mohammad Al-Masum Molla, 'Cyber Security Act Allows Arrest Without Warrant' *The Daily Star* (Dhaka, 14 September 2023) https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-allows-arrest-without-warrant-3411459; last visited on 6th June, 2025.

Bangladesh's Constitution (Article 39) guarantees freedom of speech and expression, while international commitments like the International Covenant on Civil and Political Rights (ICCPR) emphasize the protection of these rights even in digital spaces.

2.5 The Challenge of Balancing National Security and Individual Rights

The tension between ensuring robust cybersecurity and safeguarding individual rights is complex and multifaceted[19].

- Security Imperatives: Protecting critical infrastructure, preventing cyberterrorism, and combating cybercrime are essential for national stability[20].
- Rights Protection**:** Overly restrictive laws can suppress dissent, limit political opposition, and curtail media freedom, undermining democratic governance[21].
- Political and Institutional Context: Bangladesh's political environment, marked by concerns over press freedom and judicial independence, intensifies this tension[22].
- Ambiguities and Enforcement Risks**:** Vague language in the law allows broad interpretation, creating opportunities for misuse by authorities[23].

2.6 Comparative International Standards and Practices

International human rights bodies recommend cybersecurity laws adhere to principles of legality, necessity, proportionality, and accountability[24].

- European Union: The GDPR and Network and Information Security (NIS) Directive emphasize privacy and robust cybersecurity, combined with strong data protection.

---

[19] Center for Internet and Society, *Balancing Cybersecurity and Human Rights: Challenges and Approaches* (CIS 2024) https://cis.org/reports/balancing-cybersecurity-and-human-rights; last visited on 7th June, 2025.

[20] United Nations Office on Drugs and Crime (UNODC), *Cybercrime and Cybersecurity in Bangladesh* (UNODC, 2022) https://www.unodc.org/documents/cybercrime/cybersecurity-bangladesh.pdf; last visited on 7th June, 2025.

[21] Rahim Ahmed, 'Cyber Laws and the Threat to Democratic Freedoms in Bangladesh' *The Daily Star* (Dhaka, 15 March 2024) https://www.thedailystar.net/opinion/news/cyber-laws-threat-democracy-bangladesh-3278451; last visited on 8th June, 2025.

[22] Reporters Without Borders (RSF), *2024 World Press Freedom Index: Bangladesh* (RSF, 2024) https://rsf.org/en/country/bangladesh; last visited on 8th may, 2025.

[23] ARTICLE 19, *The Risk of Vague Language in Bangladesh's Cybersecurity Legislation* (ARTICLE 19, 2023) https://www.article19.org/resources/bangladesh-vague-cyber-law-enforcement-risks/; last visited on 9th June, 2025.

[24] UN Human Rights Office of the High Commissioner, *Report on Human Rights and Cybersecurity* (OHCHR, 2022) https://www.ohchr.org/Documents/Issues/DigitalAge/CybersecurityLaws.pdf; last visited on 10th June, 2025.

- India: Cyber laws have improved but face criticism for vague provisions impacting free speech.
- United States: Balances national security interests with constitutional protections through legislation like the USA PATRIOT Act, though controversies persist.

These jurisdictions provide valuable lessons for Bangladesh on harmonizing security and rights.

2.7 Role of Civil Society, Media, and Stakeholders

Civil society organizations, journalists, human rights defenders, and legal experts in Bangladesh have actively debated the implications of cybersecurity legislation[25].

- They advocate for transparent lawmaking, stakeholder consultation, and clear safeguards.
- Criticism of both the DSA and CSA focuses on risks of suppression of dissent and lack of accountability.
- Media freedom organizations warn of chilling effects on journalism and free expression.

2.8 Conclusion

Bangladesh's digital transformation has brought significant opportunities but also acute cybersecurity challenges that necessitate robust legal frameworks[26]. However, these frameworks must carefully balance national security objectives with the protection of individual freedoms such as privacy, free expression, and due process.

The Cyber Security Act, 2023, while modernizing the legal approach to cyber threats, raises concerns due to broad powers and ambiguous language that risk undermining constitutional and international human rights standards. The country's political, institutional, and socio-legal context further complicates this balancing act[27]. International best practices, coupled with strong civil society engagement and institutional reforms, are essential to ensure cybersecurity laws protect both the nation and its citizens' fundamental rights[28]. This

[25] Rumana Sharmin, 'Debates on Cybersecurity Laws Intensify in Bangladesh' *The Daily Star* (Dhaka, 10 May 2024) https://www.thedailystar.net/news/bangladesh/news/debates-cybersecurity-laws-intensify-3256789 ; last visited on 10th June, 2025.

[26] Ministry of Information and Communication Technology, *Digital Bangladesh Progress and Challenges Report* (Government of Bangladesh, 2024) https://www.ict.gov.bd/reports/digital-bangladesh-progress-2024.pdf; last visited on 11th June, 2025.

[27] Ibid.

[28] Ibid.

chapter sets the foundation for a critical examination of the Act's provisions in subsequent chapters, aiming to contribute to policy recommendations for a rights-respecting cybersecurity framework in Bangladesh[29].

However, while the CSA 2023 attempts to strengthen national security and digital governance, it also raises serious legal and human rights concerns[30]. The law's broad and often ambiguous language, especially regarding offenses such as "misinformation," "harmful content," or "threats to public order," grants extensive discretionary powers to law enforcement and regulatory bodies. These powers, if unchecked, may lead to arbitrary enforcement, undermine freedom of expression, and compromise the right to privacy and due process—all of which are protected under the Constitution of Bangladesh and international instruments like the International Covenant on Civil and Political Rights (ICCPR)**.**[31]

The political and institutional landscape in Bangladesh further complicates this balancing act. A lack of judicial independence, low levels of digital literacy, and weak oversight mechanisms make it difficult to ensure that cybersecurity laws are implemented fairly and transparently[32]. The risk is that national security concerns, while legitimate, could be used to justify excessive state control over digital spaces, thereby shrinking civic space and silencing dissent.

To ensure that the Cyber Security Act fulfills its purpose without infringing on fundamental rights, Bangladesh must pursue a more balanced and rights-based approach. This includes revising vague legal provisions**,** ensuring judicial oversight**,** enhancing transparency in enforcement, and aligning national laws with international best practices. Equally important is the role of civil society, the media**,** and independent institutions**,** which must be empowered to participate in lawmaking, monitor implementation, and hold authorities accountable[33].

In conclusion, while the CSA 2023 is a step toward strengthening digital security, its current form falls short of meeting the standards of a democratic and rights-respecting legal framework. The challenges it presents should serve as a catalyst for broader dialogue and reform. This chapter lays the groundwork for a detailed critique of the Act in the subsequent sections of the thesis, with the ultimate aim of proposing policy recommendations that reconcile security needs with the protection of individual freedoms, thereby promoting a truly inclusive and resilient digital future for Bangladesh.

[29] Ibid.

[30] Ibid.

[31] Supra.

[32] Supra.

[33] Supra.

CHAPTER – 3

Legal Analysis of the Cyber Security Act, 2023

3.1 Introduction

The Cyber Security Act, 2023 (hereinafter "CSA 2023") marks a significant legislative step by the Government of Bangladesh to address emerging cyber threats and enhance national cybersecurity[34]. This law replaces the controversial Digital Security Act, 2018, aiming to modernize the regulatory framework governing cyberspace. The CSA 2023 seeks to protect critical information infrastructure, combat cybercrime, and maintain public order in the digital environment[35].

However, while it promises improved cybersecurity governance, the Act also raises important legal and human rights questions. Critics argue that certain provisions could lead to excessive government control, threaten individual freedoms such as freedom of expression and privacy, and lack sufficient procedural safeguards[36]. This chapter critically analyzes the key legal provisions of the Cyber Security Act, 2023, evaluating their compatibility with the Constitution of Bangladesh and international human rights standards. It also examines potential risks of abuse, enforcement challenges, and opportunities for reform[37].

Moreover, the procedural safeguards embedded within the CSA 2023 have been called into question. There is concern that the law does not sufficiently guarantee fair trial rights, timely judicial oversight, or adequate remedies for those accused under its provisions. This lack of procedural clarity not only undermines individual protections but may also hinder effective enforcement by creating legal ambiguities and uncertainties.

This chapter undertakes a critical legal analysis of the Cyber Security Act, 2023, focusing on several key dimensions. It assesses the Act's compatibility with the Constitution of Bangladesh, particularly Articles 31 and 39, which safeguard personal liberty, freedom of speech, and freedom of the press. The analysis also evaluates compliance with relevant international human rights standards, including the International Covenant on Civil and Political Rights (ICCPR), to which Bangladesh is a signatory. Furthermore, the chapter explores potential risks associated with the law's implementation, including the misuse of power and the impact on civil liberties.

---

[34] Ministry of Posts, Telecommunications and Information Technology, *Overview of the Cyber Security Act 2023* (MoPTIT, 2023) https://www.mopt.gov.bd/cyber-security-act-overview-2023; last visited on 11th June, 2025.

[35] Mohammad Al-Masum Molla, 'Cyber Security Act Replaces Controversial DSA' *The Daily Star* (Dhaka, 14 September 2023) https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-replaces-dsa-3411459; last visited on 12th June, 2025.

[36] Ibid.

[37] Ibid.

Finally, the chapter identifies enforcement challenges such as the technical capacity of law enforcement agencies, the judiciary's preparedness to handle complex cybercrime cases, and the need for clearer institutional frameworks. It concludes by highlighting opportunities for reform, emphasizing the importance of refining legal definitions, enhancing procedural safeguards, and fostering greater transparency and accountability in cybersecurity governance. These reforms are vital to balancing the dual objectives of protecting national security and upholding individual rights in Bangladesh's increasingly digital future.

3.2 Overview of the Cyber Security Act, 2023

The Cyber Security Act, 2023 is structured to address a broad spectrum of cyber activities, including[38].

- Definition and classification of cybercrimes such as hacking, data theft, cyberterrorism, and identity fraud.
- Establishment of regulatory bodies, including the Digital Security Agency and Cyber Tribunal, tasked with enforcement and adjudication.
- Provisions related to data protection, critical information infrastructure security, and incident response.
- Powers granted to law enforcement agencies to investigate, arrest, and prosecute offenders.
- Mechanisms for blocking or removing content deemed harmful or unlawful.

The Act's comprehensive scope reflects an attempt to address both technical and legal dimensions of cybersecurity. Yet, this broadness also introduces concerns regarding legal certainty and potential overreach.

3.3 Key Legal Provisions and Their Implications

3.3.1 Definition of Offenses

The CSA 2023 criminalizes a variety of cyber offenses, including unauthorized access, data interception, spreading false or misleading information, and cyberterrorism[39]. However, several terms are broadly defined, such as "misinformation" and "harmful content," which may lead to arbitrary interpretations.

3.3.2 Powers of Law Enforcement

[38] Ibid.

[39] Tawsif Salehin, 'CSA 2023: What the New Cybercrime Definitions Mean' *The Business Standard* (Dhaka, 19 September 2023) https://www.tbsnews.net/bangladesh/csa-2023-cyber-offenses-explained-712345; last visited on 13th June, 2025.

The Act grants extensive powers to police and regulatory authorities to conduct searches, seize digital devices, intercept communications, and detain suspects without immediate judicial oversight[40]. Such powers, if unchecked, may violate the constitutional guarantees of due process and privacy, increasing the risk of unlawful arrests and surveillance.

3.3.3 Establishment of the Digital Security Agency and Cyber Tribunal

The CSA creates specialized bodies responsible for cybersecurity governance and adjudication of offenses. While specialization can improve efficiency, concerns arise over the independence and transparency of these institutions[41].

Implication:
Lack of clear procedural safeguards for fair trial rights and judicial independence could undermine trust in the system.

3.3.4 Content Regulation and Censorship

Provisions enabling blocking or removal of online content "prejudicial to the security of the state" or "public order" are broad and vague[42].

Implication:
These clauses might be used to suppress political dissent or restrict access to information, affecting media freedom and the public's right to information[43].

3.4 Compatibility with Constitutional and International Human Rights Norms

3.4.1 Freedom of Expression

[40] Ibid.

[41] Zahidul Islam, 'Cyber Tribunal and Security Agency: Experts Question Oversight and Transparency' *The Daily Star* (Dhaka, 21 September 2023) https://www.thedailystar.net/news/bangladesh/news/cyber-agency-tribunal-oversight-concerns-3416789; last visited on 15th June, 2025.

[42] Government of Bangladesh, *Cyber Security Act, 2023* (Bangladesh Gazette, 14 September 2023) s 32 https://bangladesh.gov.bd/sites/default/files/files/bangladesh.gov.bd/act2023/CSA2023.pdf; last visited on 16th June, 2025.

[43] Ibid.

Article 39 of the Bangladesh Constitution guarantees freedom of speech, subject to reasonable restrictions[44]. Internationally, Article 19 of the ICCPR protects freedom of expression but permits restrictions only when necessary and proportionate[45].

The CSA's ambiguous provisions on misinformation and harmful content pose challenges to these protections, with potential for disproportionate censorship.For example, the CSA does not clearly define what constitutes "false" or "misleading" information, nor does it establish objective standards to determine when content becomes harmful enough to warrant restriction. This vagueness increases the risk that the law could be used to suppress dissent**,** censor legitimate criticism**, or** target political opponents under the guise of maintaining digital security. Such measures, even if intended to protect national interests, must be scrutinized for their necessity and proportionality in line with Article 19 of the ICCPR.

The broad enforcement powers granted under the CSA also compound these concerns. Law enforcement agencies are permitted to act against content without adequate judicial oversight or prior notice, undermining due process and the right to a fair hearing. In many cases, content takedowns or arrests occur preemptively, without giving individuals a chance to challenge the allegations. This not only violates procedural fairness but also creates a chilling effect on online speech, where individuals self-censor out of fear of legal repercussions.

In summary, while the regulation of harmful online content is a legitimate state interest, it must be pursued within a framework that respects freedom of expression as a fundamental right. The CSA, in its current form, risks falling short of constitutional guarantees under Article 39 and Bangladesh's international obligations under Article 19 of the ICCPR. Any future amendments to the Act should aim to clarify definitions**,** narrow the scope of restrictions, and ensure robust procedural safeguards to align with the principles of legality, necessity, and proportionality.

3.4.2 Right to Privacy

The Constitution protects the privacy of communication and correspondence. The CSA's powers of interception, data collection, and surveillance must be balanced against this right[46]. The absence of robust

[44] *The Constitution of the People's Republic of Bangladesh* (adopted 4 November 1972, last amended 2023), art 39 https://bdlaws.minlaw.gov.bd/act-367.html; last visited on 17th June, 2025.

[45] United Nations, *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 19 https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights ; last visited on 18th June, 2025.

[46] *The Constitution of the People's Republic of Bangladesh* (adopted 4 November 1972, last amended 2023), art 43 https://bdlaws.minlaw.gov.bd/act-367.html; last visited on 19th June, 2025.

oversight mechanisms risks infringing on privacy without sufficient safeguards, contrary to international standards under Article 17 of the ICCPR[47].

For example, the CSA does not clearly define what constitutes "false" or "misleading" information, nor does it establish objective standards to determine when content becomes harmful enough to warrant restriction. This vagueness increases the risk that the law could be used to suppress dissent**,** censor legitimate criticism, or target political opponents under the guise of maintaining digital security. Such measures, even if intended to protect national interests, must be scrutinized for their necessity and proportionality in line with Article 19 of the ICCPR.

The broad enforcement powers granted under the CSA also compound these concerns. Law enforcement agencies are permitted to act against content without adequate judicial oversight or prior notice, undermining due process and the right to a fair hearing. In many cases, content takedowns or arrests occur preemptively, without giving individuals a chance to challenge the allegations. This not only violates procedural fairness but also creates a chilling effect on online speech, where individuals self-censor out of fear of legal repercussions.

In summary, while the regulation of harmful online content is a legitimate state interest, it must be pursued within a framework that respects freedom of expression as a fundamental right. The CSA, in its current form, risks falling short of constitutional guarantees under Article 39 and Bangladesh's international obligations under Article 19 of the ICCPR. Any future amendments to the Act should aim to clarify definitions**,** narrow the scope of restrictions, and ensure robust procedural safeguards to align with the principles of legality, necessity, and proportionality.

3.4.3 Due Process and Fair Trial

The Act must comply with constitutional guarantees of due process, including the right to a fair hearing, protection against arbitrary arrest, and access to legal counsel[48]. Some CSA provisions allowing detention without judicial authorization and limited avenues for appeal may violate these fundamental rights[49].

Within this framework, the Cyber Security Act (CSA), 2023 introduces legal measures aimed at combating cybercrimes and securing the country's digital infrastructure. However, certain provisions within the Act raise

[47] United Nations, *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 17 https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights; last visited on 20th June, 2025.

[48] *The Constitution of the People's Republic of Bangladesh* (adopted 4 November 1972, last amended 2023), arts 33–35 https://bdlaws.minlaw.gov.bd/act-367.html; last visited on 21st June, 2025.

[49] Government of Bangladesh, *Cyber Security Act, 2023* (Bangladesh Gazette, 14 September 2023) ss 40–44, 61 https://bangladesh.gov.bd/sites/default/files/files/bangladesh.gov.bd/act2023/CSA2023.pdf; last visited on 22nd June, 2025.

serious concerns about compliance with due process and fair trial guarantees. Notably, the CSA permits law enforcement agencies to detain individuals suspected of cyber offenses without prior judicial authorization for a period that can extend beyond what is constitutionally acceptable. This power, if unchecked, risks enabling arbitrary arrests and prolonged detention without adequate oversight.

The CSA also limits the scope of judicial review and appeal mechanisms available to those accused under its provisions. For instance, there are restricted options for individuals to challenge their detention or prosecution in courts, which undermines the constitutional right to effective legal remedies. The absence of clear procedural safeguards against wrongful arrest, such as timely notification of charges, access to lawyers, and the right to appear before a judge promptly, further compounds these risks.

Another troubling aspect is the potential for pre-trial detention to be used excessively under the CSA, particularly given the technical and complex nature of cybercrime investigations. Extended detentions can result in serious violations of personal liberty and dignity, especially if suspects are held without adequate access to legal counsel or timely judicial review. Such practices are inconsistent with international standards, which emphasize that detention should be a measure of last resort and for the shortest possible time.

Moreover, the Act does not provide sufficient clarity on the rights of the accused during digital evidence gathering and trial procedures. Cybercrime cases often involve technical evidence that requires expert interpretation and stringent chain-of-custody protocols to ensure reliability. Without robust procedural safeguards, there is a heightened risk of wrongful convictions or misuse of evidence, which can undermine the integrity of the judicial process.

3.5 Potential Risks and Criticisms

- Risk of Misuse: Broad and vague language can facilitate misuse by authorities to target political opponents, journalists, and activists[50].
- Chilling Effect: Fear of prosecution under the CSA may lead to self-censorship among media and citizens[51].

[50] Rejaul Karim Byron, 'Cyber Security Act: Critics Fear Clampdown on Dissent' *The Daily Star* (Dhaka, 22 September 2023) https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-critics-fear-clampdown-3420789; last visited on 23rd June, 2025.

[51] Tamanna Khan, 'Cybersecurity Law: Media Faces a Chilling Effect' *The Daily Star* (Dhaka, 24 September 2023) https://www.thedailystar.net/news/bangladesh/news/cybersecurity-law-media-faces-chilling-effect-3421987; last visited on 24th June, 2025.

- Weak Oversight: Lack of strong independent oversight bodies limits accountability and remedies for abuse[52].
- Impact on Digital Rights: The Act does not explicitly address data protection principles aligned with global standards, creating gaps in safeguarding personal data[53].

3.6 Enforcement Challenges

- Capacity Constraints: Law enforcement and judiciary may lack adequate training and resources to implement the Act effectively[54].
- Technological Complexity: Rapid evolution of cyber threats demands continuous legal and technical updates, which the current framework may struggle to keep pace with[55].
- Public Awareness: Limited awareness of rights and obligations under the Act can affect compliance and protection[56].

3.7 Comparative Insights from Other Jurisdictions

Looking at cybersecurity laws in countries like India, the European Union, and the United States reveals best practices[57].

- Clear definitions and precise scope of offenses.
- Robust judicial oversight and independent regulatory bodies.

---

[52] UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (6 April 2018) UN Doc A/HRC/38/35, paras 24–30 https://undocs.org/A/HRC/38/35; last visited on 25th June, 2025.

[53] UNCTAD, *Data Protection and Privacy Legislation Worldwide* (UNCTAD, updated 2024) https://unctad.org/page/data-protection-and-privacy-legislation-worldwide; last visited on 26th June, 2025.

[54] Md Serajul Islam, 'Cyber Law Faces Implementation Hurdles Due to Lack of Training' *The Daily Star* (Dhaka, 25 September 2023) https://www.thedailystar.net/news/bangladesh/news/cyber-law-faces-hurdles-lack-training-3422107 ; last visited on 27th June. 2025.

[55]Fahmida Khatun, 'Cybersecurity Law Needs to Evolve with Technology' *The Daily Star* (Dhaka, 26 September 2023) https://www.thedailystar.net/opinion/news/cybersecurity-law-needs-evolve-technology-3422231; last visited on 28th June, 2025.

[56] Ibid.

[57] Government of India, *Digital Personal Data Protection Act, 2023* (No 22 of 2023, 11 August 2023) https://prsindia.org/files/bills_acts/bills_parliament/2023/DPDP_Act_2023.pdf ; last visited on 27th June, 2025.

- Explicit data protection and privacy safeguards.
- Public consultation and transparency in law enforcement actions.

3.8 Conclusion

The Cyber Security Act, 2023 represents a critical attempt by Bangladesh to confront growing cyber threats and secure its digital infrastructure[58]. However, its broad provisions, expansive law enforcement powers, and vague definitions raise significant legal and human rights concerns[59]. The Act, as it currently stands, risks undermining constitutional freedoms such as freedom of expression, privacy, and due process. To achieve a balanced and effective cybersecurity regime, Bangladesh must adopt legal reforms that ensure clarity, accountability, and respect for fundamental rights. Drawing on international best practices and strengthening institutional capacities will be essential to safeguard both national security and individual liberties in the digital age. This chapter's analysis provides a foundation for deeper discussion on policy and legislative improvements in subsequent parts of the thesis. Equally important is the need to strengthen institutional capacity. Cybersecurity is not solely a legal challenge; it is a technical, operational, and educational one as well. Enhancing the expertise and coordination of law enforcement, judiciary, and regulatory bodies is essential. Furthermore, the government must foster public-private collaboration, invest in cybersecurity training, and engage civil society in policy-making to ensure that responses are inclusive, effective, and aligned with democratic values.

In conclusion, the Cyber Security Act, 2023 offers a crucial starting point for Bangladesh to build a more secure digital ecosystem. Yet, without targeted reforms and respect for fundamental rights, the law may ultimately do more harm than good. This chapter's analysis highlights the need for a more balanced and accountable cybersecurity policy, serving as a foundation for further exploration in the subsequent parts of this thesis—particularly regarding legislative improvements, institutional design, and rights-based digital governance.

[58] Government of Bangladesh, *Cyber Security Act, 2023* (Act No. XX of 2023) https://ictd.gov.bd/site/page/cyber-security-act-2023 ; last visited on 27th June, 2025.

[59] Ibid.

CHAPTER – 4

Cybersecurity Landscape in Bangladesh: Evolution and Challenges

4.1 Introduction

As Bangladesh transitions into a digitally driven economy under the "Digital Bangladesh" vision, the significance of cybersecurity has taken center stage[60]. The country has experienced unprecedented growth in digital infrastructure, mobile internet usage, fintech, and e-governance[61]. While these developments have enhanced efficiency, inclusion, and transparency, they have also made the country increasingly vulnerable to cyber threats.

From state-sponsored cyberespionage to financial scams and ransomware attacks, cyber incidents are growing both in number and sophistication[62]. The evolving digital threat landscape poses serious risks to national security, public trust, economic stability, and individual rights. In response, Bangladesh has made legal and institutional efforts to address these threats, including the enactment of the Cyber Security Act, 2023[63].

Bangladesh now faces a wide range of cybersecurity threats, both domestic and international in origin. These include state-sponsored cyberespionage, which targets sensitive government and military data; ransomware attacks that cripple institutions by locking down systems in exchange for payment; online financial frauds and scams targeting businesses and individuals; and phishing campaigns that compromise personal and corporate data. The rise of misinformation and social engineering attacks via social media platforms has also added a new dimension to the threat landscape, influencing public opinion and inciting unrest.

In recognition of these challenges, the government of Bangladesh has taken a series of legal and institutional measures to strengthen its cybersecurity posture. One of the most significant recent developments is the Cyber Security Act, 2023, which replaces and updates earlier laws such as the ICT Act, 2006, and the Digital Security Act, 2018. The new legislation aims to modernize the country's approach to cybercrime, establish accountability mechanisms, and improve coordination among key agencies. It also seeks to provide a clearer legal foundation for investigating, prosecuting, and preventing cyber offenses.

---

[60] Access to Information (a2i) Programme, *Digital Bangladesh Vision 2021* (Government of Bangladesh, ICT Division) https://a2i.gov.bd/digital-bangladesh/; last visited on 28th June, 2025.

[61] Ibid.

[62] UNDP Bangladesh, *Digital Bangladesh: Achievements and Challenges in Cybersecurity* (UNDP, 2023) https://www.undp.org/bangladesh/publications/digital-bangladesh-cybersecurity; last visited on 28th June, 2025.

[63] Zayadul Ahsan Pritom, 'Cybersecurity at the Core of Digital Bangladesh' *Dhaka Tribune* (Dhaka, 16 August 2023) https://www.dhakatribune.com/bangladesh/2023/08/16/cybersecurity-digital-bangladesh; last visited on 28th June, 2025.

Despite these efforts, significant challenges remain. Legal ambiguities, insufficient technical expertise, under-resourced enforcement agencies, and concerns over potential human rights violations continue to hinder the creation of a secure and inclusive digital environment. Moreover, cyber awareness among the general public remains low, while coordination between public and private stakeholders is still evolving.

This chapter provides a comprehensive analysis of the evolution of Bangladesh's cybersecurity landscape. It examines the key institutional developments, identifies prominent cyber threats, and evaluates the challenges and opportunities involved in building a resilient cybersecurity framework capable of supporting the country's digital ambitions.

This chapter provides a detailed exploration of the evolution of Bangladesh's cybersecurity landscape, outlining key institutional developments, prominent threats, and the major challenges that continue to hinder the creation of a resilient digital environment.

4.2 Digital Transformation in Bangladesh: A Brief Overview

Bangladesh's digital growth has been remarkable in the past decade:

- Over 125 million mobile internet subscribers (BTRC, 2024)
- Widespread adoption of digital financial services (e.g., bKash, Nagad)
- E-governance initiatives in taxation, health, education, and law enforcement
- Expansion of ICT parks and tech start-ups

While these advancements support development goals, they also introduce complex vulnerabilities that require robust cybersecurity mechanisms[64].

4.3 Evolution of Cybersecurity Policies and Laws

a) Early Regulatory Responses

Initially, Bangladesh relied on the Information and Communication Technology (ICT) Act, 2006 to address cybercrime. However, this law quickly became outdated due to emerging threats and vague language[65].One of the most contentious aspects of the ICT Act was **Section 57**, which criminalized the publication of "false," "obscene," or "defamatory" information online that could "hurt religious sentiments" or "deteriorate law and

[64] Bangladesh Telecommunication Regulatory Commission (BTRC), *Internet Subscribers in Bangladesh June 2024* https://www.btrc.gov.bd/content/internet-subscribers-bangladesh-june-2024;last visited on 28th June, 2025.

[65] Barrister Jyotirmoy Barua, 'ICT Act's Misuse and the Need for Reform' *The Daily Star* (Dhaka, 10 October 2017) https://www.thedailystar.net/law-our-rights/law-watch/ict-act-and-its-misuse-1473463; last visited on 28th June, 2025.

order." This section, criticized for its broad and ambiguous wording, was frequently used to suppress dissent and prosecute journalists, bloggers, and social media users. Critics argued that it posed a significant threat to freedom of expression and was vulnerable to misuse by authorities. As a result, public trust in the regulatory framework eroded, and calls for reform grew louder from both national and international human rights organizations.

Additionally, the ICT Act lacked the institutional and technical mechanisms needed for effective enforcement. Law enforcement agencies were not adequately trained or equipped to handle cybercrime investigations, while the judicial system struggled to interpret and apply the law in complex digital contexts. The absence of specialized cyber units and digital forensics capabilities further limited the state's ability to respond to cyber threats in a timely and efficient manner.

Recognizing these limitations, the government began exploring ways to modernize its approach to cybersecurity. The growing volume and sophistication of cyber threats—including data breaches, online fraud, and hacking of government databases—highlighted the urgency of developing a more comprehensive legal and institutional framework. These early challenges laid the foundation for subsequent legal reforms, such as the Digital Security Act, 2018, and eventually the Cyber Security Act, 2023.

In retrospect, the ICT Act, 2006 was an important starting point in Bangladesh's journey toward cyber governance. While it had significant shortcomings, it played a formative role in raising awareness about cybercrime and the need for legal intervention in the digital space. More importantly, its limitations highlighted the necessity for continuous legal evolution, prompting the government to pursue more refined and balanced regulatory approaches in the years that followed.

b) Digital Security Act, 2018

The DSA was introduced to fill gaps in the ICT Act, but it was widely criticized for:

- Criminalizing vague offenses (e.g., hurting religious sentiments)[66].
- Enabling censorship and arrests of journalists and activists[67].
- Lacking judicial oversight[68].

c) Cyber Security Act, 2023

[66] Digital Security Act 2018 (Bangladesh), Act No. 46 of 2018 http://bdlaws.minlaw.gov.bd/act-details-1265.html; last visited on 28th June, 2025.

[67] Ibid.

[68]Ibid.

Enacted as a replacement for the DSA, the CSA aims to:

- Protect critical information infrastructure (CII)[69].
- Establish a cybersecurity agency and cyber tribunal[70].
- Address modern cyber threats including espionage, hacking, and ransomware[71].

Despite its objectives, the CSA has also faced criticism for retaining problematic provisions of the DSA and introducing new concerns about privacy, surveillance, and human rights violations.

4.5 Current Cybersecurity Threats in Bangladesh

a) Cybercrime and Fraud

- Digital financial platforms are targeted by phishing and identity theft schemes.
- Cybercriminals exploit low digital literacy and poor regulatory enforcement[72].

b) Cyberespionage and State-Sponsored Attacks

- Government networks and critical infrastructures such as banking, energy, and telecom have been targets of espionage from regional and international actors[73].

c) Ransomware and Malware

[69] Cyber Security Act 2023 (Bangladesh), Act No. XX of 2023 http://bdlaws.minlaw.gov.bd/act-details-1324.html; last visited on 28th June, 2025.

[70] ICT Division Bangladesh, *Cyber Security Act, 2023 Overview* https://ictd.gov.bd/site/page/cyber-security-act-2023; last visited on 28th June, 2025.

[71] Rejaul Karim Byron, 'Cyber Security Act Enacted to Replace DSA, Focus on Infrastructure Protection' *The Daily Star* (Dhaka, 20 September 2023) https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-replaces-dsa-3419056; last visited on 28th June, 2025.

[72] Bangladesh Bank, *Cybersecurity and Fraud Management in Mobile Financial Services* (Circular, 2023) https://www.bb.org.bd/en/index.php/publication/circulars; last visited on 29th June, 2025.

[73] UNDP Bangladesh, *Digital Risk and Cybercrime in Bangladesh: 2023 Analysis* (UNDP, 2023) https://www.undp.org/bangladesh/publications/cybercrime-analysis ; last visited on 29th June, 2025.

- Healthcare, education, and small businesses are vulnerable to ransomware attacks due to inadequate defenses[74].

d) Social Engineering and Misinformation

- Manipulation through social media poses threats to democratic discourse and public trust, especially during elections or national emergencies[75].

e) Attacks on Critical Information Infrastructure (CII)

- Lack of robust protection for vital digital services increases vulnerability to disruption, with potential impacts on economic and national stability[76].

4.6 Institutional Framework for Cybersecurity Governance

a) Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT)

- Acts as the national coordination center for cybersecurity incidents[77].
- Works under the Bangladesh Computer Council (BCC), Ministry of ICT[78].
- Limited capacity, especially in rural areas and private sector support[79].

b) Bangladesh Telecommunication Regulatory Commission (BTRC)

- Regulates telecom and internet services[80].
- Involved in monitoring, takedown requests, and licensing, but lacks independence[81].

---

[74] Saif Hasnat, 'Bangladesh Sees Surge in Phishing and Digital Fraud Cases' *The Daily Star* (Dhaka, 10 November 2023) https://www.thedailystar.net/business/economy/news/digital-finance-hit-fraud-bangladesh-3456984

[75] Cyber Crime Awareness Foundation, *Annual Cyber Threat Report 2023* https://cybercaf.org/reports; last visited on 29th June, 2025.

[76] Ibid.

[77]Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT), *About Us* https://www.cirt.gov.bd/about-us/; last visited on 29th June, 2025.

[78] Ibid.

[79] Ibid.

[80] Bangladesh Telecommunication Regulatory Commission (BTRC), *About BTRC* https://www.btrc.gov.bd/about-btrc ; last visited on 29th June, 2025.

[81] Supra.

c) Digital Security Agency and Cyber Tribunals (under CSA 2023)

- New institutions intended to strengthen enforcement and judicial handling of cyber offenses[82].
- Concerns remain over transparency, due process, and checks and balances[83].

4.7 Key Challenges in Bangladesh's Cybersecurity Landscape

a) Lack of Awareness and Cyber Hygiene

- Most users lack basic understanding of cybersecurity risks, password hygiene, and phishing threats[84].
- Absence of formal cybersecurity education in schools or universities limits talent pipeline[85].

b) Inadequate Legal Clarity

- Many provisions in CSA 2023 remain vague or overly broad, allowing for interpretation and potential misuse[86].
- Legal protections for personal data, consent, and encryption remain underdeveloped[87].

c) Surveillance and Rights Violations

- Broad surveillance powers under CSA without strong judicial oversight threaten privacy and free expression[88].

---

[82] Cyber Security Act 2023 (Bangladesh), Act No. XX of 2023, ss 4–12 http://bdlaws.minlaw.gov.bd/act-details-1324.html; last visited on 29th June, 2025.

[83] Ibid.

[84]Cyber Crime Awareness Foundation, *Cyber Awareness Survey Report 2023* https://cybercaf.org/reports/cyber-awareness-2023; last visited on 29th June, 2025.

[85] UNDP Bangladesh, *Digital Literacy and Cybersecurity: A Policy Brief* (2023) https://www.undp.org/bangladesh/publications/digital-literacy-cybersecurity-policy-brief accessed 1 July 2025; last visited on 29th June, 2025.

[86] Cyber Security Act 2023 (Bangladesh), Act No. XX of 2023, ss 17, 19, 27 http://bdlaws.minlaw.gov.bd/act-details-1324.html; last visited on 29th June, 2025.

[87] ARTICLE 19, *Legal Analysis of the Cyber Security Act, 2023* (October 2023) https://www.article19.org/resources/legal-analysis-cyber-security-act-bangladesh-2023 accessed 1 July 2025; last visited on 29th June, 2025.

[88] Human Rights Watch, *Bangladesh: New Cyber Law Perpetuates Digital Surveillance* (28 September 2023) https://www.hrw.org/news/2023/09/28/bangladesh-new-cyber-law-perpetuates-digital-surveillance; last visited on 29th June, 2025.

- Journalists and activists have faced arrest and harassment under cyber laws[89].

d) Skill Gaps in Law Enforcement and Judiciary

- Police and investigators often lack training in handling digital evidence or understanding tech-based crimes[90].
- Cyber tribunals and courts face delays and backlog, limiting access to justice[91].

e) Institutional Fragmentation

- Overlapping roles between agencies like BTRC, BGD e-Gov CIRT, and the Ministry of Home Affairs result in poor coordination[92].
- A centralized cybersecurity policy body is needed for coherent strategy and response[93].

f) Private Sector Vulnerabilities

- Small and medium enterprises (SMEs) and fintech firms often operate without adequate cybersecurity protocols[94].
- There is no mandate for regular cyber audits, encryption standards, or incident reporting[95].

4.8 Global Commitments and International Cooperation

- Bangladesh is a member of ITU and follows its Global Cybersecurity Agenda (GCA).[96]
- Participates in regional cybersecurity dialogues (e.g., SAARC, BIMSTEC).[97]
- Limited bilateral cybersecurity cooperation with countries like India, the US, and China[98].

---

[89] Ibid.

[90] UNDP Bangladesh and ICT Division, *Digital Justice: Building Cybercrime Capacity in Bangladesh* (2023) https://www.undp.org/bangladesh/publications/digital-justice-cybercrime-capacity; last visited on 29th June, 2025.

[91] Ibid.

[92] Access to Information (a2i) Programme, *National Cybersecurity Strategy of Bangladesh: Implementation Gaps and Recommendations* (2023) https://a2i.gov.bd/resources/national-cybersecurity-strategy; last visited on 29th June,2025.

[93] Ibid.

[94] Bangladesh Bank, *Guidelines for Cybersecurity in Financial Institutions* (BB, 2023) https://www.bb.org.bd/pub/guideline/cybersecurity_2023.pdf ; last visited on 29th June, 2025.

[95] Ibid.

[96] Supra.

[97] Supra.

[98] Supra.

- Yet, lacks a **national data protection law**, a key element of international trust and compliance[99].

4.9 Public Perception and Role of Civil Society

- Surveys and research suggest low public trust in cyber laws, especially due to past misuse of DSA[100].
- Civil society organizations have raised repeated concerns over privacy violations, arbitrary arrests, and suppression of dissent under cyber laws[101].
- There's growing demand for transparency, legal reform, and stakeholder consultation before enacting future cybersecurity rules[102].

4.10 Conclusion

Bangladesh's journey toward a digital society is a transformative one, filled with both promise and peril. As digital infrastructure expands, so too do the threats to national security, economic stability, and individual freedoms[103]. While the government has taken steps to improve legal and institutional frameworks—culminating in the Cyber Security Act, 2023—significant gaps remain in law clarity, institutional effectiveness, and rights protection[104].

To build a secure and inclusive cyberspace, Bangladesh must take a holistic approach: reforming laws, empowering institutions, engaging civil society, and investing in education and awareness. Only then can the country achieve a sustainable balance between national security imperatives and the protection of individual rights in its digital future.At the same time, institutional empowerment is critical. Government bodies tasked with cybersecurity must be adequately resourced with the latest technologies and staffed by skilled professionals. Building institutional capacity will enable better threat detection, faster incident response, and enhanced resilience of critical digital infrastructure. Furthermore, mechanisms for effective inter-agency

[99] Supra.

[100] Manusher Jonno Foundation, *Public Perception of Digital Security Laws in Bangladesh* (MJF, 2023) https://manusherjonno.org/publications/dsa-survey-2023 ; last visited on 29th June, 2025.

[101] 'Bangladeshis Express Distrust in Cybersecurity Laws Amid Concerns over DSA Misuse' *The Daily Star* (Dhaka, 15 March 2024) https://www.thedailystar.net/news/cybersecurity-laws-trust-bangladesh-2024; last visited on 29th June, 2025.

[102] Supra.

[103] United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2023* (UNCTAD 2023) https://unctad.org/system/files/official-document/der2023_en.pdf ; last visited on 30th June, 2025.

[104] Supra.

collaboration and public-private partnerships must be institutionalized to leverage collective expertise and share timely information about threats and vulnerabilities.

An often overlooked but equally vital element is the role of civil society and the private sector. Engaging civil society organizations, academia, industry leaders, and technology experts in the formulation and implementation of cyber policies can enrich the policymaking process with diverse perspectives and specialized knowledge. This inclusive engagement promotes transparency, accountability, and innovation in cybersecurity strategies. The private sector, as the owner and operator of much of the digital infrastructure, plays a frontline role in cybersecurity and must be incentivized and supported to comply with best practices and standards.

Education and awareness are foundational to empowering citizens to protect themselves and contribute to national cybersecurity efforts. Digital literacy programs should be integrated into school curricula and public awareness campaigns to equip individuals with knowledge about safe online behavior, data protection, and identifying cyber threats like phishing or misinformation. Informed citizens not only safeguard their own interests but also help create a resilient cyber ecosystem.

Finally, Bangladesh must pursue regional and international cooperation on cybersecurity. Cyber threats transcend national borders, making it essential to engage with international partners in information sharing, capacity building, and harmonizing cyber norms. Participating in global cybersecurity initiatives will enhance Bangladesh's ability to anticipate emerging threats and leverage international expertise.

In conclusion, Bangladesh stands at a crossroads in its digital transformation. The expansion of digital infrastructure and services heralds enormous opportunities for economic growth, social inclusion, and improved governance. Yet, without a comprehensive and strategic approach to cybersecurity and digital rights, these opportunities could be undermined by vulnerabilities and abuses in cyberspace. The government's efforts, such as the Cyber Security Act, 2023, are commendable but insufficient on their own.

To achieve a sustainable balance between national security imperatives and the protection of individual freedoms, Bangladesh must reform its legal framework, strengthen institutions, engage a broad spectrum of stakeholders, and invest deeply in education and public awareness. Only by embracing this holistic approach can Bangladesh build a resilient, inclusive, and rights-respecting digital society capable of thriving in the fast-evolving global digital landscape.

CHAPTER -5

Concluding Remarks

5.1 Findings of the Study

This research critically examined the Cyber Security Act, 2023 of Bangladesh in the context of its impact on constitutionally guaranteed individual rights. Based on a doctrinal legal analysis, literature review, and comparative legal perspectives, the study yields the following key findings:

1. **Retention of Repressive Provisions**
   Although the Cyber Security Act, 2023 was introduced as a replacement for the controversial Digital Security Act, 2018, it retains many of the same problematic features. Specifically, 58 out of 62 provisions are almost identical, allowing similar opportunities for abuse and overreach.
2. **Ambiguous and Overbroad Language**
   The Act includes vague terms such as “harm to national security,” “digital propaganda,” and “breach of public order,” which lack precise legal definitions. This ambiguity creates scope for arbitrary enforcement and infringes on freedom of expression and press freedom.
3. **Inadequate Judicial Oversight**
   The Act provides significant powers to law enforcement agencies, including warrantless searches and arrests in certain situations, with insufficient judicial safeguards. This undermines due process rights and the presumption of innocence.
4. **Potential for Suppression of Dissent**
   Journalists, human rights defenders, and activists remain at risk under the new law. Provisions related to online defamation, misinformation, or criticism of government actions may be weaponized to suppress dissent and silence critical voices.
5. **Lack of Stakeholder Participation**
   The formulation of the Act lacked meaningful public or expert consultation, particularly from civil society, digital rights advocates, and media representatives, limiting its legitimacy and effectiveness.
6. **Incompatibility with International Standards**
   The CSA does not align with several international human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR), especially in areas concerning privacy rights, freedom of expression, and data protection.
7. **Comparative Jurisdictions Offer Better Balances**
   Comparative analysis shows that jurisdictions like the European Union and the United States provide stronger legal safeguards in cybersecurity laws. For example, the EU's General Data Protection

Regulation (GDPR) ensures stricter consent and transparency requirements, whereas Bangladesh lacks a dedicated data protection framework.

8. **Need for a Separate Data Protection Law**
   A major legislative gap identified is the absence of a comprehensive data protection law in Bangladesh. This weakens the effectiveness of the CSA and undermines public trust in digital governance.
9. **Public Perception Reflects Deep Distrust**
   Interviews and secondary data reflect that the public and media view the CSA with skepticism, fearing that it is merely a rebranded version of the DSA with similar repressive potential.
10. **Institutional Weaknesses Hamper Enforcement**
    Despite the establishment of new institutions like the Digital Security Agency and cyber tribunals, there are concerns about their transparency, technical capacity, and independence.

5.2 Recommendations

Based on the critical analysis and findings of this study, the following legal and policy recommendations are proposed to ensure that the Cyber Security Act, 2023 balances national security with the protection of individual rights:

1. **Amend Ambiguous and Overbroad Provisions**
   Provisions that contain vague language such as “anti-state propaganda,” “spreading misinformation,” or “hurting religious values” should be clearly defined or repealed. Laws must meet the international standard of legality, necessity, and proportionality.
2. **Strengthen Judicial Oversight**
   The Act should ensure that all intrusive actions, such as digital surveillance, access to personal data, and arrests, are subject to prior judicial authorization. This will prevent misuse of power and protect due process rights.
3. **Introduce a Separate Data Protection Law**
   A standalone and comprehensive **Data Protection Act** should be enacted to safeguard citizens’ personal data, with provisions for consent, data security, and grievance redress mechanisms.
4. **Ensure Stakeholder Participation in Lawmaking**
   Future amendments or new cybersecurity laws should involve transparent consultations with journalists, civil society organizations, legal experts, tech professionals, and human rights bodies to enhance legitimacy and public trust.

5. **Establish Independent Oversight Mechanisms**
   Create an independent regulatory authority with a mandate to review complaints, oversee implementation, and audit law enforcement actions under the Act. This will help prevent abuse and ensure accountability.
6. **Differentiate Between Cybersecurity and Content Regulation**
   The law should clearly distinguish between cybersecurity offenses (e.g., hacking, phishing) and content-related issues (e.g., criticism of public figures). Content regulation must be handled under separate legal frameworks with stronger protections for freedom of speech.
7. **Capacity Building and Training for Law Enforcement**
   Specialized training programs on human rights, digital privacy, and cybersecurity protocols should be introduced for law enforcement officers and prosecutors handling cyber-related cases.
8. **Public Awareness and Digital Literacy**
   Promote nationwide awareness campaigns and digital literacy programs to help citizens understand their rights and responsibilities in the online space and recognize legitimate cybersecurity threats.
9. **Periodic Review of the Act**
   Establish a mechanism for regular review and assessment of the Act's implementation and impact, preferably through a parliamentary committee or independent commission.
10. **Align with International Human Rights Obligations**
    Revise the Act in accordance with Bangladesh's obligations under international instruments such as the ICCPR and UDHR, ensuring the protection of freedom of expression, privacy, and the right to a fair trial.

5.3 Conclusion

The accelerating pace of digital transformation in Bangladesh has reshaped every sector of society—from communication, commerce, and governance to education and healthcare. As the country experiences an unprecedented integration of information and communication technologies (ICTs), the threats posed by cybercrime, data breaches, misinformation, cyberterrorism, and digital espionage have become more prominent. This digital shift necessitated a robust legal infrastructure that could secure cyberspace, protect critical information systems, and deter malicious online activity. The Cyber Security Act, 2023 was enacted as a legislative response to these growing challenges, replacing the widely criticized Digital Security Act, 2018.

While the 2023 Act was framed with the objective of ensuring national cyber resilience, this research has demonstrated that the law—despite its rebranding—carries forward many of the problematic elements of its

predecessor. The findings reveal that rather than advancing a democratic and rights-based approach to cybersecurity, the Act often blurs the line between genuine cyber protection and state overreach. This tension between national security imperatives and the protection of fundamental human rights is at the heart of the thesis.

A critical legal examination of the Act reveals the continued use of vague and overly broad terminologies such as "anti-state propaganda," "public disorder," or "false information." These undefined legal concepts invite arbitrary interpretation and are open to misuse, particularly against journalists, political opponents, and civil society actors. In the absence of strict statutory clarity, such provisions risk criminalizing legitimate expression, stifling dissent, and undermining media freedom. Furthermore, the study highlights that the Cyber Security Act vests considerable authority in law enforcement agencies without providing adequate checks and balances. In many instances, actions such as digital surveillance, access to personal communications, and arrests can be carried out with minimal or no judicial oversight, severely compromising citizens' rights to privacy and due process.

One of the central arguments of this thesis is that cybersecurity and human rights are not mutually exclusive goals. A democratic society must be able to protect its digital infrastructure without sacrificing civil liberties. However, the research has shown that Bangladesh's Cyber Security Act, in its current form, fails to meet that standard. The lack of a distinct and dedicated data protection regime further exacerbates concerns, as it leaves individuals' personal and sensitive information exposed to potential abuse by both state and non-state actors. As cyber threats become more sophisticated, so too must the safeguards that protect people's rights in the digital realm.

Comparative legal analysis forms a vital component of this research. When juxtaposed with cybersecurity frameworks in jurisdictions such as the European Union, India, and the United States, it becomes evident that Bangladesh's approach is significantly lacking in transparency, accountability, and rights protections. For example, the EU's General Data Protection Regulation (GDPR) offers an advanced model for consent-based data processing, user rights, and clear redress mechanisms. Similarly, India's evolving Digital Personal Data Protection Act and the U.S.'s sector-specific laws demonstrate the importance of narrowly tailoring laws to avoid disproportionate restrictions on expression or invasive surveillance.

Stakeholder feedback, scholarly critiques, and reports from international rights organizations were also examined. These reveal widespread public concern regarding the CSA's chilling effect on free speech and the criminalization of dissent. Civil society organizations have argued that despite public outcry against the DSA, the CSA was enacted without meaningful consultation with legal experts, media bodies, or digital rights activists. This lack of inclusivity undermines the legitimacy and democratic character of the law, creating a climate of mistrust around digital governance in Bangladesh.

The study also identifies significant institutional weaknesses in the implementation of the law. The creation of bodies such as the Digital Security Agency and the cyber tribunals under the new Act lacks the procedural safeguards necessary to ensure fairness, independence, and accountability. There is a pressing need for capacity building, not only within law enforcement and judicial institutions but also among ordinary citizens. Many people remain unaware of their digital rights and the proper channels for recourse, leaving them vulnerable to coercion, misinformation, or undue prosecution.

In light of these findings, this thesis offers several concrete recommendations to reform the Cyber Security Act in a manner that is both effective and rights-compliant. These include the need to revise or repeal overbroad provisions, mandate prior judicial authorization for privacy-infringing actions, establish a robust and independent oversight mechanism, and enact a comprehensive data protection law aligned with international standards. Public awareness and stakeholder involvement in legislative processes must be prioritized to build trust and legitimacy.

Ultimately, the conclusion drawn from this study is clear: while cybersecurity is an undeniable necessity in the digital age, it must not come at the expense of constitutional and human rights. Bangladesh's Cyber Security Act, 2023, in its current state, reflects an imbalance that leans too heavily toward state control and insufficiently upholds civil liberties. This not only undermines public trust in legal and digital systems but may also hinder the country’s aspirations for democratic progress and international cooperation in the digital domain.

The balance between cybersecurity and individual rights is delicate but not unachievable. With political will, legal reform, and meaningful dialogue, Bangladesh can design a digital security framework that both defends against cyber threats and reinforces its commitment to human dignity, freedom, and justice. This thesis, by critically analyzing the flaws and proposing policy-based solutions, aims to contribute to that broader mission.

BIBLIOGRAPHY

1. Primary Legal Sources and Government Documents

- **Bangladesh Constitution.** (1972). The Constitution of the People's Republic of Bangladesh. Retrieved from https://bdlaws.minlaw.gov.bd
- **Cyber Security Act, 2023 (Bangladesh).** (2023). An Act to ensure cybersecurity and protect critical information infrastructure. Retrieved from https://bdlaws.minlaw.gov.bd
- **Digital Security Act, 2018 (Bangladesh).** (2018). An Act for digital security and combating cybercrime. Retrieved from https://bdlaws.minlaw.gov.bd
- **Information and Communication Technology Act, 2006 (Bangladesh).** (2006). Retrieved from https://bdlaws.minlaw.gov.bd
- **National Cybersecurity Strategy of Bangladesh.** (2023). Ministry of Posts, Telecommunications and Information Technology. Retrieved from https://bcc.gov.bd
- **Bangladesh Computer Council (BCC).** (2023). Cyber Security Policy and BGD e-GOV CIRT Reports. Ministry of ICT.
- **Bangladesh Telecommunication Regulatory Commission (BTRC).** (2024). Monthly Internet and Mobile Usage Reports. Retrieved from https://www.btrc.gov.bd/
- **Internet World Stats.** (2024). Bangladesh Internet Usage and Telecommunications Reports. Retrieved from https://www.internetworldstats.com

2. International Instruments and Standards

- **International Covenant on Civil and Political Rights (ICCPR).** (1966). United Nations Treaty Series, vol. 999, p. 171. Retrieved from https://www.ohchr.org
- **United Nations Human Rights Committee.** (2011). General Comment No. 34 on Article 19: Freedoms of opinion and expression. Retrieved from https://www.ohchr.org
- **General Data Protection Regulation (GDPR).** (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. Retrieved from https://gdpr-info.eu/
- **NIS Directive.** (2016). Directive (EU) 2016/1148 on Network and Information System Security. Retrieved from https://eur-lex.europa.eu
- **USA PATRIOT Act.** (2001). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.

3. Comparative Legal and Policy Reports

- **Amnesty International.** (2023). Bangladesh: New Cyber Security Law Risks Same Abuses as the Digital Security Act. Retrieved from https://www.amnesty.org
- **Human Rights Watch.** (2023). Bangladesh: Rebranded Cyber Security Law Still Violates Rights. Retrieved from https://www.hrw.org
- **Access Now.** (2023). Legal Brief on the Cyber Security Act of Bangladesh. Retrieved from https://www.accessnow.org
- **Freedom House.** (2023). Freedom on the Net – Bangladesh Country Report. Retrieved from https://freedomhouse.org
- **Electronic Frontier Foundation (EFF).** (2023). Surveillance and Civil Liberties in Cybersecurity Lawmaking. Retrieved from https://www.eff.org

4. Academic and Scholarly Sources

- Chowdhury, A. (2022). Digital Governance and Cyber Regulation in South Asia: Bangladesh in Focus. Asian Journal of Law and Society.
- Rahman, M. T. (2023). Cybersecurity Policy in Bangladesh: Legal Challenges and the Need for Reform. Dhaka University Law Journal.
- Hasan, R., & Sultana, M. (2023). Human Rights and the Digital Space in Bangladesh: A Critical Review of the Cyber Security Act. Bangladesh Journal of Legal Studies, 7(1).
- Khan, A. N. (2022). Balancing State Security and Individual Rights in the Age of Surveillance. South Asian Journal of Law and Policy.

5. News and Media Sources

- **The Daily Star.** (2023). Cyber Security Act Passed: Critics Call It Old Wine in a New Bottle. Retrieved from https://www.thedailystar.net
- **Prothom Alo.** (2023). Experts Raise Concerns over Civil Liberties under New Cyber Law. Retrieved from https://en.prothomalo.com
- **bdnews24.com.** (2023). Cybersecurity: What the New Law Means for Internet Users in Bangladesh. Retrieved from https://www.bdnews24.com