An Assignment on

Building a Resilient Digital Future: Proposing Legal Reforms for Cyber Law in Bangladesh Based on Leading Global Examples

An Assignment submitted to the Department of Computer Science and Engineering,
Hajee Mohammad Danesh Science and Technology University

Course Title: Computer Ethics and Cyber Law
Course Code: CSE 455

Submitted To,
Pankaj Bhowmik
Lecturer
Department of Computer Science and Engineering

Submitted By,
Md. Gaosul Azam Mridul
Student ID: 2002047
Level 4, Semester II

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
HAJEE MOHAMMAD DANESH SCIENCE AND TECHNOLOGY UNIVERSITY,
DINAJPUR-5200, BANGLADESH

1. Introduction

The rapid integration of digital technologies into everyday life in Bangladesh has sparked a transformative shift across all sectors—from education, healthcare, and finance to agriculture, public administration, and national security. With over 130 million internet users and an ever-growing digital economy, Bangladesh is poised to reap substantial benefits from the fourth industrial revolution. However, this digital proliferation also exposes the country to an increasing range of cybersecurity risks, data breaches, online fraud, digital misinformation, and emerging technological threats like deepfakes and artificial intelligence misuse.

While Bangladesh has made strides in enacting laws like the Digital Security Act (DSA) 2018, there remains a significant gap between legal frameworks and the real-world challenges of a complex and interconnected digital society. Current legislation lacks the necessary provisions for data protection, robust cybersecurity standards, and clear delineation of rights and responsibilities among digital stakeholders. Furthermore, the absence of legal clarity and accountability in the DSA has sparked public concerns over freedom of expression and privacy rights.

To safeguard digital sovereignty, protect civil liberties, and foster innovation, Bangladesh must now adopt a holistic and forward-looking approach to cyber law reform. This includes benchmarking against international standards, contextualizing global best practices to fit the local socio-economic and legal landscape, and ensuring that reform efforts are inclusive, transparent, and enforceable. This assignment explores global models of effective cyber legislation and proposes actionable reforms aimed at creating a resilient and adaptive digital future for Bangladesh.

2. Current State of Cyber Law in Bangladesh

Bangladesh's primary cyber legal instrument is the Digital Security Act (DSA) 2018. While it aims to curb cybercrime, it has drawn criticism for vague definitions, potential misuse, and infringement on freedom of expression.

Key Issues:

- Ambiguity in definitions of cybercrime
- Lack of clarity on data protection
- Inadequate provisions for digital evidence and cybersecurity standards
- Concerns about human rights and freedom of speech

3. Global Cyber Law Frameworks: Leading Examples

3.1 European Union(EU)

- **General Data Protection Regulation(GDPR, 2016/679)**

  The EU has some of the strongest data protection laws:

  - Comprehensive data protection law
  - Emphasis on consent, transparency, and accountability
  - Rights to access, rectify, and erase personal data

3.2 European Union (EU)

- **CLOUD ACT(2018)**
- **NIST Cybersecurity Framework**

  - Promotes cross-border data sharing with legal safeguards
  - NIST Framework provides voluntary guidelines for critical infrastructure cybersecurity
  - Encourages sector-specific compliance and public-private cooperation

3.3 Singapore

- **Cybersecurity Act 2018**
  - Secures Critical Information Infrastructure (CII)
  - Mandates reporting of cyber incidents
  - Introduces licensing for cybersecurity service providers

3.4 India

- **Information Technology Act(2000)**
- **Digital Personal Data Protection Act(2023)**
  - Regulates intermediaries and electronic governance
  - New data protection law introduces roles for data fiduciaries
  - Focuses on digital consent and storage localization

3.5 Australia

- **Privacy Act 1988(Amended)**
- **Security of Critical Infrustucture Act 2018**
  - Strong data privacy requirements
  - Powers to oversee and intervene in critical infrastructure cybersecurity
  - Mandatory data breach notifications

3.6 Canada

- **Personal Information Protection and Electronic Documents Act(PIPEDA)**
  - Federal privacy law governing private-sector data handling
  - Obligates organizations to secure personal information and notify breaches
  - Proposed replacement: Consumer Privacy Protection Act (CPPA)

3.7 South Korea

- **Personal Information Protection Act(PIPA, 2011)**

  - Recognized as one of the strictest data privacy laws in Asia
  - Requires data minimization and prior consent
  - Independent Personal Information Protection Commission

4. Cyber Law in Bangladesh

The main law in Bangladesh is the Digital Security Act (DSA), 2018. It covers issues like:

- Hacking and unauthorized access
- Cyberbullying and online harassment
- Digital fraud and spreading false information

It also created organizations like the Digital Security Agency and BGD e-GOV CIRT to respond to cyber threats.
Problems with DSA:

- It contains vague definitions that can be misused.
- It allows arrest without a warrant in some cases.
- It is often used to suppress freedom of speech, especially against journalists.
- It lacks modern data protection measures.

5. Proposing Legal Reforms for Cyber Law in Bangladesh

Based on global examples, the following reforms are suggested:

5.1 Data Protection Law

- Introduce a standalone Data Protection Act
- Establish a Data Protection Authority (DPA)
- Define rights of data subjects
- Include data breach notification obligations

5.2 Syber Security Standards and Frameworks

- Develop national cybersecurity standards modeled on NIST or ISO/IEC 27001
- Regular audits for public and private digital systems
- Enforce risk assessment and breach reporting obligations

5.3 Digital Rights and Freedom of Expression

- Amend DSA 2018 for clear, narrow definitions of offences
- Ensure judicial oversight for surveillance and content regulation
- Enshrine protections for journalistic and academic speech

5.4 Capacity Building and Awareness

- Promote nationwide cybersecurity education and training
- Support local development of security tools and innovation
- Raise awareness about privacy rights and safe digital practices

5.5 Cybercrime Investigation and Forensics

- Establish specialized cybercrime units with technical expertise
- Invest in digital forensic laboratories and tools
- Ensure proper chain of custody and admissibility of digital evidence

5.6 Regulation of Artificial Intelligence and Emerging Technologies

- Create legal definitions and categories for AI and automated decision-making systems
- Mandate ethical AI design and transparency in algorithmic decision-making
- Provide oversight on biometric and facial recognition technologies

5.7 Protection of Critical Information Infrastructure(CII)

- Identify and classify national critical infrastructure sectors (e.g., energy, health, finance)
- Enforce risk-based regulations and mandatory security audits
- Impose incident reporting requirements for CII operators

5.8 International Cooperation and Mutual Legal Assistance

- Join global treaties such as the Budapest Convention on Cybercrime
- Establish mutual legal assistance agreements (MLATs) for transnational investigations
- Develop frameworks for cross-border data transfer and jurisdictional clarity

5.9 Consumer Protection in E-Commerce and Fintech

- Strengthen consumer data rights and dispute resolution mechanisms
- Regulate online platforms and payment services for fraud prevention
- Impose liability standards for online service providers

5.10 Whistleblower Protection and Transparency

- Enact laws to protect cybersecurity whistleblowers from retaliation
- Encourage anonymous reporting channels for breaches and illegal surveillance
- Ensure transparency in public procurement of surveillance tools

6. Conclusion

Bangladesh stands at a critical juncture where digital growth must be matched with legal preparedness. By learning from global leaders and tailoring solutions to local needs, Bangladesh can build a resilient digital future that safeguards its citizens and empowers innovation. Effective legal reforms will not only enhance national security and economic competitiveness but also strengthen human rights and public trust in the digital ecosystem.

7. References

- EU GDPR: https://gdpr.eu/
- US CLOUD Act: https://www.justice.gov/cloudact
- US NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
- Singapore Cybersecurity Agency: https://www.csa.gov.sg
- India Digital Personal Data Protection Act: https://www.meity.gov.in/
- Australia Privacy Act: https://www.oaic.gov.au/privacy/privacy-legislation/privacy-act
- Canada PIPEDA: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
- South Korea PIPA: https://www.pipc.go.kr