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,
Kanij Fatema
Student ID: 2002023
Level 4, Semester II

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

1. Introduction

The digital world is growing every day, and people are using the internet more than ever. Along with these benefits, there are also risks. Cybercrimes like hacking, data theft, online scams, fake news, and privacy violations are becoming more common. These threats are not just harmful to individuals but also affect companies, governments, and the whole society. To protect people and systems in the digital space, countries make laws called cyber laws.

Some countries like the United States, United Kingdom, China, Australia, India, and members of the European Union (EU) have created strong and modern cyber laws to handle digital crimes and protect data. Bangladesh also has a cyber law known as the Digital Security Act, 2018. But many experts say this law needs to be improved to deal with current and future challenges. This paper compares Bangladesh's cyber law with leading global examples and gives suggestions for how to make it better. The goal is to build a safe and strong digital future for Bangladesh.

2. Global Cyber Law Frameworks: Leading Examples

2.1 United States

The United States has several cyber laws that are spread across different areas:

- The Computer Fraud and Abuse Act (CFAA) punishes hacking and unauthorized access.
- The Cybersecurity Information Sharing Act (CISA) allows companies to share threat information with the government.
- Special laws like HIPAA and GLBA protect data in the health and financial sectors.
- The NIST Cybersecurity Framework offers rules and suggestions for improving cyber safety.

These laws focus on public-private cooperation and protecting data in different sectors [1].

2.2 European Union (EU)

The EU has some of the strongest data protection laws:

- The General Data Protection Regulation (GDPR) gives people full control over their personal data and applies even to companies outside Europe.
- The Network and Information Systems (NIS) Directive forces critical infrastructure operators to adopt security measures.

These laws are known for being strict and clear about data rights and responsibilities [2].

2.3 United Kingdom

The UK has:

- The Data Protection Act 2018, which follows GDPR standards.
- The Computer Misuse Act 1990, which punishes cybercrimes.
- A National Cyber Strategy focusing on awareness, security, and innovation.

The UK's approach balances security, privacy, and innovation [3].

2.4 India

India's main law is the Information Technology (IT) Act 2000, updated in 2008. It:

- Criminalizes cybercrimes such as hacking, identity theft, and cyber terrorism.
- Legally recognizes digital documents and signatures.
- Has an agency called CERT-IN to handle cyber emergencies.

India is also working on a new Digital Personal Data Protection Bill [4].

2.5 China

China has a strict and state-controlled system of cyber laws:

- The Cybersecurity Law (2017) requires network operators to store data within China and protect personal information.
- The Data Security Law (2021) and Personal Information Protection Law (2021) govern how data is used and stored.
- The Chinese model emphasizes state control and national security over user freedom.

China's laws focus more on controlling information than on individual privacy [5].

2.6 Australia

Australia's approach includes both security and transparency:

- The Cybercrime Act 2001 punishes crimes like hacking and online fraud.
- The Privacy Act 1988, recently updated, governs how organizations collect and use personal data.
- The Australian Cyber Security Centre (ACSC) handles national cyber protection.

Australia also introduced a Cyber Security Strategy 2023–2030, aiming to become a world leader in cybersecurity [6].

3. 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.

4. Proposing Legal Reforms for Cyber Law in Bangladesh

Based on global examples, the following reforms are suggested:

4.1 Create a Separate Data Protection Law

- Like the EU's GDPR or India's draft bill, Bangladesh should have a separate Data Protection Act.
- An independent Data Protection Authority (DPA) should be created.
- The law should define rights, duties, and penalties for data misuse.

4.2 Improve the Digital Security Act (DSA)

- Remove unclear and abusive sections.
- Define all cybercrimes and procedures clearly.
- Introduce judicial oversight to prevent misuse.

4.3 Strengthen Cyber Institutions

- Give more power and resources to BGD e-GOV CIRT.
- Create a National Cybersecurity Council to make policies and handle big threats.

4.4 Encourage Business Participation

- Make laws for information sharing between businesses and the government.
- Provide tax benefits for companies that follow cybersecurity standards.

4.5 Improve Public Awareness

- Start training programs for government officers.
- Include cyber education in schools and universities.

4.6 Join International Treaties

- Bangladesh should join the Budapest Convention on Cybercrime.

- Sign agreements with other countries for faster cooperation in fighting cross-border cybercrime.

5. Conclusion

Cybersecurity is a critical part of national security and public safety. Bangladesh must update its laws to meet the demands of a digital world. By learning from the United States, EU, UK, China, Australia, and India, Bangladesh can create a legal system that protects both people and institutions. These reforms will help ensure a secure, trusted, and resilient digital future for everyone in Bangladesh.

6. References

[1] U.S. Department of Justice. "Computer Fraud and Abuse Act (CFAA)." https://www.justice.gov/

[2] European Union. "General Data Protection Regulation (GDPR)." https://gdpr.eu/

[3] UK Government. "Data Protection Act 2018." https://www.legislation.gov.uk/

[4] Ministry of Electronics and IT, India. "Information Technology Act, 2000." https://www.meity.gov.in/

[5] Cyberspace Administration of China. "Cybersecurity and Data Protection Laws." http://www.cac.gov.cn/

[6] Australian Government. "Cyber Security Strategy 2023–2030." https://www.cyber.gov.au/