An Assignment on

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

Course Code: CSE 455

Course Title: Computer Ethics and Cyber Law

Submitted By

Md. Ahad Ali

Student ID: 2002035

Session: 2019-20

Submitted To

Pankaj Bhowmik

Lecturer

Department of CSE, HSTU



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

HAJEE MOHAMMAD DANESH SCIENCE AND TECHNOLOGY UNIVERSITY, DINAJPUR-5200, BANGLADESH

May 2025

**Abstract**

As Bangladesh moves forward in its digital development, it faces growing threats such as data breaches, online scams, fake news, and cyberattacks. The main laws currently in place—the ICT Act 2006 and the Digital Security Act 2018—are outdated and not clear enough to deal with today’s challenges. This paper looks at the weaknesses in these laws and suggests a plan to improve them. By learning from successful examples in the European Union, the United States, and Singapore, this paper offers a set of reforms tailored to Bangladesh. These reforms aim to create a safe online environment that protects people’s data, encourages innovation, and meets international standards. Key ideas include better legal definitions, independent watchdog bodies, and training for those enforcing the law.

**Chapter 1**

**Introduction**

In today's world, digital technology plays a major role in almost every area of life—government, business, education, and healthcare. While this creates many opportunities, it also brings serious cyber risks. Cyber laws are crucial for protecting people online, setting rules for digital behavior, and punishing online crimes.

In Bangladesh, projects like “Digital Bangladesh” have helped increase internet use and digital services. But along with this growth, there are increasing risks like hacking, identity theft, online harassment, and attacks on important infrastructure. The current laws are not strong or clear enough to deal with these new dangers.

This paper will review the current cyber laws in Bangladesh, compare them with effective international laws, and suggest legal updates that match the country’s needs. The goal is to help Bangladesh become a secure and forward-thinking digital nation.

**Chapter 2**

**Current Situation of Cyber Law in Bangladesh**

**2.1 Main Laws:**

ICT Act 2006: Created to handle online transactions and crimes. But it's now outdated, with confusing and overlapping rules.

Digital Security Act 2018: Designed to update cyber laws, but criticized for being too vague and giving too much power to law enforcement.

**2.2 Main Problems:**

Unclear Definitions: Words like “digital crime” or “data” are not well explained, making the law hard to apply.

Jurisdiction Issues: Bangladesh struggles to deal with cybercrimes that happen across borders due to a lack of international agreements.

No Data Protection Law: There’s no strong law to protect people’s private information.

Human Rights Concerns: The Digital Security Act is sometimes used to silence critics, threaten journalists, and invade privacy, often without court approval.

**Chapter 3**

**Examples of Effective Cyber Laws from Other Countries**

**3.1 European Union – GDPR:**

* The General Data Protection Regulation (GDPR) is the world’s strongest data protection law.
* Key Points:
* Users must give clear permission before their data is used.
* Companies must report data breaches within 72 hours.
* People have the right to delete or move their data.
* Companies can be heavily fined (up to 4% of their yearly income) if they don’t follow the rules.

**3.2 United States – CFAA & CISA:**

* CFAA (Computer Fraud and Abuse Act) focuses on stopping illegal access to computers.
* CISA (Cybersecurity Information Sharing Act) encourages sharing information between government and private companies to fight cyber threats.
* Focuses on protecting critical services, quick reporting, and protecting those who share info in good faith.

**3.3 Singapore – Cybersecurity Act 2018:**

* A strong, centralized system for national cyber protection.
* Key Features:
* Identifies and protects important systems like power, water, and banking.
* Requires licenses for cybersecurity professionals.
* Makes reporting of serious cyber incidents mandatory.
* Sets up constant monitoring and fast response plans.

**Chapter 4**

**Suggested Reforms for Bangladesh’s Cyber Law**

**4.1 Clearer Terms and Broader Coverage:**

Define important terms like “cybercrime,” “personal data,” and “digital evidence.”

Include modern cyber threats like phishing, ransomware, crypto scams, and AI-driven attacks.

**4.2 Data Protection Law:**

* Create a new Data Protection Act based on the GDPR.
* Set up a separate Data Protection Authority (DPA) with the power to investigate and act.
* Protect individual rights:
* People must give informed consent before their data is used.
* People can access, change, or delete their personal data.
* People can limit how their data is used.

**4.3 Cybersecurity Readiness and Reporting Rules:**

* Set minimum cybersecurity standards for key sectors.
* Require regular cybersecurity checks for important organizations.
* Create a National Cyber Incident Response Team (NCIRT) for quick action.
* Penalize companies that don’t report big cyber incidents.

**4.4 International Help and Local Training:**

* Join global agreements like the Budapest Convention on Cybercrime.
* Make agreements with other countries to share information and investigate crimes.
* Train judges, lawyers, and investigators in cyber law.
* Build forensic labs and set clear rules for digital evidence.

**4.5 Balancing Security and Human Rights:**

* Ensure court oversight before conducting surveillance.
* Protect journalists and whistleblowers from unfair arrest.
* Make enforcement transparent through public reports and reviews.
* Include civil society, tech companies, and universities in making laws.

**Chapter 5**

**How to Make the Reforms Happen**

**5.1 Step-by-Step Plan:**

Step 1: Update legal terms, create the DPA, and pass a data protection law.

Step 2: Build the NCIRT, define important systems, and start audits.

Step 3: Fully launch surveillance oversight and start international partnerships.

**5.2 Involving Stakeholders:**

Talk to:

* Tech groups like BASIS and BCS
* Lawyers and rights organizations
* International experts and donors
* Get public feedback through online platforms.

**5.3 Raising Awareness and Education:**

* Use social media, TV, and schools to educate people.
* Teach digital rights in school curriculums.
* Offer online courses on cybersecurity basics.

**5.4 Strengthening Institutions:**

* Train BTRC staff, police cyber teams, and judges.
* Fund special cybercrime courts and investigation teams.
* Create a national dashboard to track cyber threats and trends.

**Conclusion**

For Bangladesh to lead in the digital world, it must have strong, clear, and fair cyber laws. The digital future depends on building trust, protecting rights, and encouraging innovation. By adopting proven strategies from other countries and adapting them to local needs, Bangladesh can create a safe and successful digital environment.

These suggested reforms fill current legal gaps and prepare the country for future technology changes and global cooperation. A safer digital Bangladesh is not only a national goal but also part of being a responsible global player.

**References**

[1] Government of Bangladesh, \*Information and Communication Technology (ICT) Act\*, 2006.

[2] Government of Bangladesh, \*Digital Security Act\*, 2018.

[3] European Union, \*General Data Protection Regulation (GDPR)\*, 2016.

[4] United States Congress, \*Computer Fraud and Abuse Act (CFAA)\*, 1986.

[5] United States Congress, \*Cybersecurity Information Sharing Act (CISA)\*, 2015.

[6] Parliament of Singapore, \*Cybersecurity Act\*, 2018.

[7] United Nations Office on Drugs and Crime (UNODC), \*Comprehensive Study on Cybercrime: Draft\*, 2013.

[8] International Telecommunication Union (ITU), \*Global Cybersecurity Index Reports\*, various years.

[9] INTERPOL, \*Cybercrime Annual Reports\*, various years.

[10] World Bank, \*Cybersecurity Readiness Assessments\*, various years.

[11] \*International Journal of Cyber Criminology\*, various issues.

[12] \*Cybersecurity Law Review\*, various issues.