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

Rafia Tusnim Oeshi
ID-2909029074
Level-4 Semester -ll

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

Abstract

As Bangladesh advances toward a digitally integrated society, the importance of resilient cyber laws becomes paramount. However, outdated regulations, enforcement inefficiencies, and lack of data protection have exposed the country's digital infrastructure to significant risks. This paper evaluates Bangladesh's current cyber legal framework and proposes actionable legal reforms by drawing from successful global models in the United States, European Union, Estonia, and Singapore. The goal is to create a robust, secure, and rights-respecting digital environment for all citizens.

Introduction

Introduce the digital transformation of Bangladesh under "Digital Bangladesh" vision. Explain the growing importance of cybersecurity in governance, economy, and personal privacy. Highlight global cyber threats such as hacking, ransomware, data theft, and disinformation. Emphasize the need for updated, rights-based, and globally aligned cyber laws. Thesis statement: This assignment critically examines Bangladesh's cyber legal framework, compares it with leading global practices, and proposes viable legal reforms to ensure digital resilience.

Current Cyber Law Landscape in Bangladesh

Overview of Laws

ICT Act, 2006: Origins, purpose, and major provisions.

Digital Security Act, 2018: Objectives, key sections (Section 21, 25, 29, 31), and controversies.

Other related acts: Penal Code, Evidence Act, Information Act, etc.

Institutional Framework

Bangladesh Telecommunication Regulatory Commission (BTRC)

Digital Security Agency (DSA)

National Data Center

Key Issues

Lack of a **comprehensive data protection law**

Overreach and misuse of laws (impact on freedom of expression)

Weak enforcement and cybersecurity preparedness

Lack of awareness and digital literacy among citizens and businesses

No unified cybersecurity strategy or CERT structure

Global Cyber Law Benchmarks: Comparative Analysis

United States

NIST Cybersecurity Framework

Federal and State-level laws (e.g., CCPA, HIPAA)

Role of CISA (Cybersecurity & Infrastructure Security Agency)

Emphasis on sector-specific, risk-based approaches

European Union

General Data Protection Regulation (GDPR): consent, rights, breach notification, data minimization

NIS Directive: Cybersecurity obligations for critical sectors

Focus on data sovereignty and privacy

Singapore

Cybersecurity Act 2018: Critical Information Infrastructure (CII) protection

Smart Nation Initiative and IMDA's regulatory role

Collaboration between public and private sectors

Estonia

Fully digital government and e-Residency program

X-Road: decentralized data exchange platform

Emphasis on citizen rights and digital identity

Advanced cyber defense coordination via CCDCOE

Legal Reform Proposals for Bangladesh

Drafting a New Data Protection Law

Inspired by GDPR: Right to access, correct, delete, portability, breach notification

Establish a **Data Protection Authority (DPA)**

Reforming the Digital Security Act

Remove ambiguous clauses that infringe on rights (e.g., Sections 25, 29)

Define clear boundaries for state surveillance and law enforcement access

Establishing a National Cybersecurity Framework

Based on NIST model: Identify, Protect, Detect, Respond, Recover

Setup of **Bangladesh Computer Emergency Response Team (BD-CERT)**

Strengthening Institutional Roles

Empower BTRC with cybersecurity mandate

Create cybercrime courts and forensic labs

Promoting Public-Private Partnership

Incentives for private companies to comply with cybersecurity standards

Shared threat intelligence platforms

Enhancing Digitade cl Literacy & Awareness

Nationwiybersecurity awareness campaigns

Integration into school/university curricula

Challenges to Implementation

Political resistance: Fear of reducing government control

Institutional weakness: Capacity, corruption, coordination gaps

Lack of funding for cybersecurity infrastructure

Public mistrust due to previous misuse of laws

Balancing security and freedom in a developing democracy

Conclusion and Recommendations

Recap: Cybersecurity is a national priority in the digital age.

Legal reforms must be inclusive, transparent, and in line with global standards.

Bangladesh must:

Enact a data protection law

Reform rights-restricting clauses

Adopt a national cybersecurity framework

Build capacity at institutional and citizen levels

Emphasize international collaboration, tech diplomacy, and rights-based policymaking.

Final remark: Building digital trust is foundational for sustainable digital progress.

References

(Use APA/MLA/Chicago format as per instructions. Suggested sources include:)

Digital Security Act, 2018 (Bangladesh Government Gazette)

General Data Protection Regulation (GDPR), European Commission

NIST Cybersecurity Framework

Singapore Cybersecurity Strategy Report

Estonian e-Governance Academy Whitepapers

World Bank & ITU reports on cyber governance

Scholarly articles from *Computer Law & Security Review*, *Journal of Cyber Policy.*

1.