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,
Sadia Islam Neela
Student ID: 2002070
Level 4, Semester II

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

1. Introduction : The digital revolution has transformed Bangladesh, with over 180 million mobile users and a booming fintech sector like bKash. However, cybercrimes such as hacking, phishing, and misinformation threaten this progress. The 2016 Bangladesh Bank heist, where \$81 million was stolen, exposed our vulnerabilities.

The 2024 student-led uprising, which led to Sheikh Hasina's resignation, marks a new era for democratic reforms, demanding robust cyber laws to rebuild trust and security. This paper compares Bangladesh's cyber law framework with those of five leading developed nations—United States, United Kingdom, Germany, Japan, and Canada—and proposes innovative reforms to create a resilient digital future. As a student inspired by the uprising, I aim to craft a youth-driven plan that balances security, ethics, and innovation.

2. Bangladesh's Current Cyber Legal Structure: Progress and Pitfalls

In the wake of rapid digitalization and the pressing need to address cyber threats, Bangladesh introduced the **Cyber Security Ordinance 2024**. This legislative move aimed to bolster cybersecurity measures and establish a more robust legal framework. However, while the ordinance signifies progress in certain areas, it also raises concerns regarding potential overreach and ambiguities.

Progress: Establishment of Dedicated Cybersecurity Bodies

The ordinance proposes the formation of the **National Cyber Security Agency (NCSA)** and the **National Cyber Security Council**. These bodies are envisioned to oversee cybersecurity strategies, coordinate responses to cyber incidents, and ensure the protection of digital infrastructures. The establishment of such dedicated entities indicates a structured approach to tackling cyber threats.

Pitfalls: Broad Powers and Ambiguous Provisions

One of the most contentious aspects of the ordinance is the extensive authority granted to the **Director General of the NCSA**. Under Clause 8, the Director General can request the **Bangladesh Telecommunication Regulatory Commission (BTRC)** to remove or block information deemed harmful. However, the term "appropriate cases" lacks a clear definition, leading to concerns about potential misuse and suppression of dissent.

Furthermore, the ordinance allows for **warrantless searches, seizures, and arrests** under Section 36, with reports to be submitted to a tribunal without a specified timeline. This absence of a reporting deadline increases the risk of harassment and abuse by authorities.

Despite digitization efforts, Bangladesh's legal framework remains reactive and outdated.

2.1 ICT Act 2006

- Criminalizes hacking and digital fraud.
- Criticized for misuse and vague language.
- Section 57 was repealed after backlash over free speech violations.

2.2 Digital Security Act 2018

- Expanded jurisdiction over cyber threats.
- Includes cyber tribunals and digital surveillance powers.
- **Issues**:
    - Ambiguity in definitions.
    - Potential use against journalists and activists.
    - Lacks clarity on AI, biometric data, and international cooperation.

Case in Point: In the 2021 Prothom Alo defamation case, the DSA was criticized for being used to silence journalists, rather than protect citizens from real digital threats.

3. Legal Frameworks in Developed Countries

3.1 United States

- **Laws**: CFAA, CCPA, Patriot Act.
- Emphasis on protecting critical infrastructure and citizen data.
- Controversial NSA surveillance exposed by Edward Snowden in 2013.

3.2 United Kingdom

- GDPR-aligned laws (post-Brexit version of Data Protection Act).
- National Cyber Security Centre (NCSC) coordinates defenses.
- Strict protocols for corporate breaches.

3.3 Germany

- GDPR with strict biometric and data surveillance limitations.
- Strong civil rights protections against algorithmic bias.

3.4 Japan

- Advanced AI regulation under APPI.
- Active in educating citizens through cybersecurity literacy campaigns.

3.5 Canada

- PIPEDA governs digital data.
- Balanced approach to privacy and innovation.
- Public-private collaboration on cybercrime detection.

4. Comparative Review: Where Bangladesh Falls Short

Issue	Bangladesh	US	UK	Germany	Japan	Canada
Data Protection	No dedicated law	CCPA	GDPR	GDPR	APPI	PIPEDA
AI Regulation	None	Draft frameworks	Developing	Ethical AI charter	National AI Strategy	AI Transparency Debates
Digital Rights	Often suppressed	Constitutionally protected	Judicially enforced	Highly protected	Strong protections	Balanced & reviewed
Youth Digital Engagement	Minimal	Strong advocacy	Digital literacy programs	University-AI Ethics Units	Youth Cyber Labs	Online Safety Commissions

5. PROPOSE Youth-Driven Reforms: Building a Democratic Cyber Future

After seeing the Cyber Security Ordinance 2024 rushed in without much public input, it's clear Bangladesh needs better, smarter cyber laws. Not just tough ones—but fair, transparent, and future-ready. Here's what we can do, based on how developed countries like the US, UK, Germany, Japan, and Canada handle it:

5.1 Add Court Permission Before Snooping

Right now, officials can check digital data without a warrant. In countries like the US and Germany, that's not allowed without a court's permission. Bangladesh should follow suit—**no one's data should be touched without a proper legal reason**.

5.2 Involve People in Making the Laws

When the UK passed its online safety law, it consulted people for months. In Bangladesh, we got

3 days to react. Future cyber laws should allow **students, techies, journalists, and even everyday users to give feedback** before it's final.

5.3 Create a Privacy Law

We don’t have a strong data privacy law yet. Europe has GDPR. Japan has one too. Bangladesh needs a proper rule that says:

i. Ask before using someone’s data
ii. Let people delete their data
iii. Inform if data leaks
iv. Punish abusers

5.4 Handle AI Threats and Deepfakes

Deepfakes and fake news are rising here. In Canada and Germany, there are new rules to stop this. We need the same—**clear laws to ban harmful AI misuse**, especially in politics and media.

5.5 Help Cybercrime Victims

Many people—especially women—face online abuse but don’t get help. We should have a **24/7 cyber helpline** with legal, emotional, and tech support. Also, schools and colleges should teach basic cyber safety.

5.6 Let Youth Co-Create Cyber Policies

Young people are online the most. Why aren’t they involved in lawmaking? Bangladesh could create a **youth-led tech policy group**, like in Estonia, to brainstorm better rules for the digital future.

5.7 Make Companies More Responsible

Big tech, banks, and mobile apps should be certified for cyber safety—like restaurants get hygiene ratings. That would build public trust.

Final Thought:

Bangladesh is changing. If we want a digital future that’s safe, fair, and innovative, we can’t just copy laws. We need to **build our own smart system—where rights, safety, and innovation grow together**.

6.Conclusion:

Bangladesh stands at a turning point. With the rise of digital connectivity, political awareness, and a bold new generation stepping forward, our cyber laws must evolve beyond control and punishment. They should protect citizens, respect privacy, and inspire innovation.

By learning from global leaders like the USA, UK, Germany, Japan, and Canada—and grounding those lessons in our own reality—we can create a cyber legal system that is both

strong and democratic. But true progress will only come if we involve the very people who live online the most: our youth.

This isn't just about fixing weak laws. It's about building a future where **digital rights are human rights**, where technology supports truth and freedom—not fear and control. Bangladesh has the potential to lead South Asia in ethical digital governance. Now is the time to take that step.

7. References

1. [1] ARTICLE 19, "Bangladesh: Digital laws must be transparent and protect free expression," *ARTICLE 19*, Mar. 5, 2024. [Online]. Available: https://www.article19.org/resources/bangladesh-digital-laws-must-be-transparent-and-protect-free-expression
2. [2] The Daily Star, "Cyber Security Ordinance 2024: Progress or Pitfall?" *The Daily Star*, Mar. 26, 2024. [Online]. Available: https://www.thedailystar.net/tech-startup/news/cyber-security-ordinance-2024-progress-or-pitfall-3785116
3. [3] Daily Sun, "Role of Youth in Building a Better Bangladesh," *Daily Sun*, Mar. 20, 2024. [Online]. Available: https://www.daily-sun.com/post/762832
4. [4] BitSight, "7 Cybersecurity Frameworks To Reduce Cyber Risk," *BitSight Blog*, Jul. 12, 2023. [Online]. Available: https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk