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,**  Mrinal Basak Shuvo  Student ID: 2002064  Level 4, Semester II |

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

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

**1. Introduction :** As the digital landscape continues to evolve, nations are facing unprecedented challenges in securing cyberspace. The emergence of artificial intelligence (AI), big data, and the Internet of Things (IoT) has accelerated both innovation and vulnerability. In Bangladesh, the digital transformation is progressing rapidly, yet the legal architecture governing cyberspace remains under-equipped to deal with modern threats like ransomware, cross-border data theft, and AI-powered misinformation.

This paper aims to explore the current state of cyber law in Bangladesh, compare it with the frameworks of top developed countries, and ultimately propose futuristic, resilient, and forward-thinking legal reforms tailored for Bangladesh. By incorporating global best practices and anticipating future threats, Bangladesh can build a digital legal framework that not only protects its citizens but also encourages ethical digital innovation.

**2. Cyber Laws in Bangladesh: Present Scenario**

Bangladesh's journey in cyber legislation has been marked by efforts to balance digital security with civil liberties. The enactment of the **Cyber Security Act (CSA) in 2023** aimed to address cybercrimes but faced criticism for retaining elements from the earlier **Digital Security Act (DSA) of 2018**, which was known for suppressing freedom of expression.

In response to public outcry and the need for reform, the **interim government introduced the Cyber Protection Ordinance (CPO) in 2024**, repealing nine controversial sections from the CSA. Notably, the CPO recognized internet access as a civil right and criminalized cyber harassment, especially against women and children.

However, concerns persist. Organizations like **Transparency International Bangladesh (TIB)** and **ARTICLE 19** have highlighted that the CPO retains vague definitions and grants broad powers to authorities without adequate judicial oversight. The rapid drafting process, with limited public consultation, has also been a point of contention.

In summary, while Bangladesh has taken steps to reform its cyber laws, ensuring transparency, precise definitions, and stakeholder engagement remains crucial to uphold digital rights and freedoms.

Bangladesh’s cyber governance is primarily shaped by two key laws:

#### ****2.1 Information and Communication Technology (ICT) Act, 2006****

* The first major cyber legislation.
* Criminalizes hacking, identity theft, and cyber pornography.
* Criticized for vague definitions and the misuse of Section 57 (later repealed).

#### ****2.2 Digital Security Act (DSA), 2018****

* Replaced controversial ICT Act sections.
* Expanded to cover crimes like digital fraud, cyberbullying, and defamation.
* **Key features**:
  + Cyber tribunals for digital offenses.
  + Provisions for real-time surveillance by law enforcement.
* **Criticism**:
  + Often considered **overly broad** and **used to suppress dissent**.
  + Lacks comprehensive guidelines on **data protection**, **AI accountability**, and **cross-border cybercrime**.

Currently, Bangladesh does **not have a separate Data Protection Act**. This gap leaves room for abuse of personal information, especially as more services move online.

### **3. Cyber Laws in Top 5 Developed Countries**

#### ****3.1 United States****

* **Laws**: Computer Fraud and Abuse Act (CFAA), Electronic Communications Privacy Act, and multiple state laws like **CCPA (California Consumer Privacy Act)**.
* **Strengths**: Focus on digital rights, data privacy, and critical infrastructure protection.
* **Innovation**: Cybersecurity and Infrastructure Security Agency (CISA) monitors national threats.

#### ****3.2 United Kingdom****

* **Laws**: Computer Misuse Act, Data Protection Act (aligned with **GDPR**).
* **Focus**: Cybercrime, data sovereignty, and citizen privacy.
* Strong collaboration with **EUROPOL** for cross-border issues.

#### ****3.3 Germany****

* Follows **GDPR** as part of the EU.
* **BSI Act** for critical infrastructure cybersecurity.
* Very strict on **biometric data**, facial recognition, and AI surveillance.

#### ****3.4 Japan****

* **Act on the Protection of Personal Information (APPI)**.
* Laws around **AI ethics**, robotics, and cybersecurity awareness in education.
* Strong private-sector partnerships for national cybersecurity.

#### ****3.5 Canada****

* **PIPEDA** (Personal Information Protection and Electronic Documents Act).
* Clear data privacy principles.
* Active role in **international cybercrime treaties** (e.g., Budapest Convention).

### **4. Bangladesh vs. Developed Countries: A Comparative Snapshot**

| **Feature** | **Bangladesh** | **USA** | **UK** | **Germany** | **Japan** | **Canada** |
| --- | --- | --- | --- | --- | --- | --- |
| **Data Protection Law** | None | CCPA | GDPR-based | GDPR | APPI | PIPEDA |
| **Cybercrime Handling** | DSA (often vague) | CFAA, CISA | Computer Misuse Act | BSI Act | Cybersecurity Strategy | Criminal Code + Treaties |
| **Surveillance Law** | Real-time monitoring by govt | NSA oversight, with backlash | Judicial oversight | Strict limits | Monitored | Balanced approach |
| **AI Regulation** | None | AI Bill of Rights (draft) | Developing | GDPR + AI ethics | Emerging AI guidelines | Algorithm transparency debates |

**5. Proposing Unique Legal Reforms for Bangladesh: A Futuristic Cyber Blueprint**

As Bangladesh accelerates towards a digitally integrated society, it must anticipate not just present threats, but also the challenges of tomorrow. Below are six forward-thinking legal reform proposals—each addressing a rising concern in the global digital ecosystem. These proposals are informed by trends in leading nations, but adapted for Bangladesh’s local realities and ambitions.

#### 5.1 ****Quantum-Safe Cybersecurity Law****

**Problem**: With the rise of quantum computing, traditional encryption methods used in banking, government, and personal communications will become vulnerable to rapid decryption.

**Proposed Reform**: Bangladesh should pass legislation requiring critical infrastructure sectors—particularly financial institutions and public services—to adopt quantum-resistant encryption standards by 2030. These standards should align with the post-quantum cryptographic guidelines being developed by the U.S. National Institute of Standards and Technology (NIST).

**Additional Measure**: Establish a Quantum Cyber Defense Research Cell under the Bangladesh e-Government initiative to develop local capabilities and collaborate internationally.

#### 5.2 ****The AI Accountability and Ethics Act****

**Problem**: The rapid deployment of artificial intelligence in decision-making—without proper regulation—raises concerns about deepfakes, algorithmic bias, and misinformation.

**Proposed Reform**: Introduce a comprehensive AI law that includes:

* Mandatory transparency audits for high-impact AI systems.
* A legally enshrined “Right to Explanation” when AI systems affect credit access, employment, or law enforcement outcomes.
* A national ban on the development and deployment of autonomous lethal AI, in line with the European Union’s draft AI Act.
* A licensing framework for AI developers in sensitive sectors such as health, security, and education.

#### 5.3 ****Personal Neurodata and Biometric Rights Law****

**Problem**: Emerging technologies that track brain activity and collect biometric data (e.g., facial recognition, voice prints) remain unregulated, risking mass surveillance and privacy violations.

**Proposed Reform**:

* Recognize “cognitive liberty”—the right to mental privacy and autonomy—as a fundamental digital right.
* Mandate explicit, informed consent for all forms of biometric and neurodata collection.
* Criminalize unauthorized biometric profiling and usage by both state and private actors.

#### 5.4 ****The Metaverse Law of 2030****

**Problem**: As virtual environments grow in scale and importance, users face new forms of harm—such as avatar impersonation, virtual asset theft, and harassment in digital spaces.

**Proposed Reform**:

* Legally recognize digital identity and virtual assets as extensions of a person’s real-world rights.
* Criminalize virtual crimes, including “avatar impersonation” and “metaverse harassment.”
* Pilot “Virtual Courts” to resolve digital disputes quickly within the environments in which they arise.

#### 5.5 ****National Digital Resilience Council (NDRC)****

**Problem**: Cybersecurity in Bangladesh currently lacks coordination, with multiple ministries and agencies operating independently.

**Proposed Reform**: Establish the National Digital Resilience Council—a multidisciplinary body including legal scholars, technologists, ethicists, cybercrime experts, and youth representatives. The council’s responsibilities would include:

* Reviewing and updating digital laws annually.
* Running simulations of digital crises to test legal and technical preparedness.
* Launching public education campaigns on digital literacy, misinformation, and cyber threats.

#### 5.6 ****Cross-Border Cyber Peace Pact****

**Problem**: Cybercrimes often originate from outside national borders, yet Bangladesh has limited regional cooperation frameworks in place.

**Proposed Reform**: Bangladesh could lead the formation of a South Asia Cyber Peace Framework in partnership with India, Sri Lanka, Nepal, and Bhutan. Key components would include:

* Joint investigation and prosecution protocols for transnational cybercrimes.
* A regional cybersecurity incident response hub, headquartered in Dhaka.
* Shared training programs for cyber law enforcement officers across the region.

These proposals are more than policy ideas—they are a blueprint for ethical innovation. If adopted, Bangladesh could become a regional leader in cyber governance, setting an example for other developing nations. In an era where digital rights are human rights, legal reform must be anticipatory, inclusive, and principled. The time for action is now.

**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>