**An Assignment on**

**Building a Resilient Digital Future: Proposing Legal Reforms for Cyber Law in**

**Bangladesh Based on Leading Global Examples**

**A logo of a science laboratory

AI-generated content may be incorrect.**

**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 By,**  **Arjon Talukder**  **Student ID: 2002022**  **Level 4, Semester II** | **Submitted To,**  **Pankaj Bhowmik**  **Lecturer**  **Department of Computer Science and**  **Engineering** |
|  |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

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

**1. Introduction**

In today's interconnected world, digital spaces are central to education, business, governance, and everyday life. As Bangladesh advances toward a digitally empowered society, its legal frameworks must evolve accordingly. This proposal outlines comprehensive legal reforms aimed at strengthening the nation’s cyber governance through a rights-based, forward-looking, and globally informed approach.

By analyzing best practices from countries such as Germany, Canada, Japan, the United Kingdom, and the United States, the proposal highlights the need for robust cyber legislation that promotes innovation, protects civil liberties, and anticipates emerging threats. These reforms are essential not only for national security but also for building trust and resilience in the digital era.

**2. Objectives of the Proposal**

The core objectives of this proposal are:

* To critically assess the existing cyber legal landscape in Bangladesh.
* To identify specific legal and structural gaps in current laws.
* To recommend progressive legal reforms that reflect international standards.
* To build a legal environment that upholds privacy, fosters trust, and protects against evolving digital risks.

These goals align with Bangladesh’s broader vision of becoming a digitally inclusive and secure society, as outlined in its Digital Bangladesh agenda and Smart Bangladesh vision.

**3. Current Legal Landscape and Global Comparison**

As Bangladesh moves toward a digitally interconnected society, the legal frameworks regulating cyberspace have grown in importance. However, while progress has been made, there remains a significant gap between the current legal provisions in Bangladesh and the comprehensive, rights-based, and future-oriented frameworks found in many developed nations. This chapter provides an overview of Bangladesh’s major cyber laws and compares them with international counterparts to highlight areas where legal reform is most urgently needed.

**3.1 Existing Cyber Laws in Bangladesh**

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

This was Bangladesh’s first comprehensive attempt at regulating cyber activities. The law aimed to address crimes such as hacking, identity theft, and digital forgery. However, it was widely criticized for vague language and misuse, particularly **Section 57**, which was often used to suppress free speech online. This section was eventually repealed, but the Act’s limitations laid the groundwork for further reform.

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

The DSA was introduced to replace problematic aspects of the ICT Act and expand the legal coverage of digital offenses. It includes provisions against cyberbullying, digital defamation, hacking, and misinformation. The Act also allowed for **real-time surveillance by authorities**, which raised serious concerns regarding privacy and freedom of expression. Human rights groups and journalists have frequently criticized the DSA for its overbroad clauses and potential for abuse.

**Cyber Security Act (CSA), 2023**

The CSA aimed to modernize the digital legal framework and align more closely with national security goals. It introduced new provisions for protecting critical infrastructure and combating cyber terrorism. However, many of its sections inherited the same issues of vagueness and limited judicial oversight as previous laws.

**Cyber Protection Ordinance (CPO), 2024**

This ordinance was introduced to address public criticism of the CSA and repeal several controversial sections. It marked a positive shift by **recognizing internet access as a civil right** and criminalizing cyber harassment, particularly against women and children. Nonetheless, legal experts have noted that definitions remain imprecise, and meaningful stakeholder consultation was largely absent in its drafting process.

**3.2 Key Challenges in Bangladesh’s Cyber Legal System**

* **Absence of a dedicated Data Protection Law:**  
  There is currently no standalone legislation that outlines how personal data should be collected, processed, stored, or shared in Bangladesh.
* **Limited AI governance:**  
  Existing laws do not address the ethical or legal implications of artificial intelligence, algorithmic bias, or machine learning applications in sensitive sectors.
* **Minimal public consultation in lawmaking:**  
  Cyber laws have historically been drafted with limited input from civil society, tech experts, or the youth—the primary users of digital platforms.
* **Over-centralization of authority:**  
  Enforcement is heavily reliant on law enforcement and intelligence agencies, often with insufficient judicial or independent oversight.

**3.3 Comparative Analysis: Bangladesh vs. Developed Countries**

To design future-ready cyber laws, it is essential to compare Bangladesh’s framework with those of countries that have implemented more comprehensive, transparent, and human-rights–centered digital legislation.

| **Aspect** | **Bangladesh** | **USA** | **UK** | **Germany** | **Japan** | **Canada** |
| --- | --- | --- | --- | --- | --- | --- |
| **Data Protection Law** | None | CCPA | Data Protection Act (GDPR-aligned) | GDPR | APPI | PIPEDA |
| **Cybercrime Law** | ICT Act, DSA, CSA | CFAA, Electronic Communications Privacy Act | Computer Misuse Act | BSI Act (Critical Infrastructure Protection) | Penal Code, APPI | Criminal Code, Cybercrime Act |
| **AI Regulation** | Not available | AI Bill of Rights (Draft) | In development | GDPR + Ethics Guidelines | Early-stage legislation | Under policy review |
| **Surveillance Oversight** | Weak | NSA oversight (Controversial) | Judicial authorization required | Strong limits under GDPR | Administrative monitoring | Balanced judicial review |
| **Public Participation** | Limited | Moderate | High | High (multi-stakeholder) | Moderate | High (public consultations) |

**3.4 Lessons for Bangladesh**

The global comparison reveals that while Bangladesh has made legislative efforts in the cyber domain, these laws often lack the scope, precision, and protections found in international frameworks. Countries like Germany and Canada have focused on citizen rights, consent-based data collection, and independent oversight. The UK and Japan emphasize transparency and early public education on cybersecurity. The USA leads in critical infrastructure protection and technological innovation, though it too faces debates around privacy.

To bridge this gap, Bangladesh must develop laws that:

* Clearly define digital rights and responsibilities.
* Incorporate judicial oversight and public input.
* Protect data with a rights-based approach.
* Regulate AI and emerging technologies with ethical safeguards.
* Embrace regional and international collaboration.

**4. Proposed Legal Reforms**

**4.1 National Data Protection and Privacy Law**

**Why it matters:**  
With increased digitization, personal data is constantly collected by governments, corporations, and digital platforms. Without a robust legal framework, this information is prone to misuse.

**Proposed actions:**

* Enact a standalone **Data Protection Act** that clearly defines what constitutes personal data and establishes legal rights for data subjects.
* Set up an **independent Data Protection Authority** to enforce compliance and manage grievances.
* Require informed, opt-in consent for all data collection, especially by online platforms and government services.

**4.2 AI Accountability and Ethical Use Law**

**Why it matters:**  
AI technologies are increasingly used in decision-making systems—such as credit scoring, hiring, and predictive policing—but without legal safeguards, they risk amplifying bias, discrimination, and misinformation.

**Proposed actions:**

* Introduce a **Right to Explanation** for individuals affected by automated decision-making.
* Mandate **algorithmic audits** and bias-testing for high-risk AI applications.
* Prohibit the deployment of **autonomous lethal AI systems**, aligning with global humanitarian guidelines.

**4.3 Quantum-Resilient Cybersecurity Framework**

**Why it matters:**  
Quantum computing poses a major threat to traditional encryption methods. Without timely preparation, critical infrastructure and sensitive data could be exposed.

**Proposed actions:**

* Require public and financial institutions to adopt **quantum-safe encryption** by 2030.
* Establish a **Quantum Cyber Defense Research Unit** under the ICT Division to promote domestic capability and international collaboration.

**4.4 Digital Rights in Virtual and Augmented Environments**

**Why it matters:**  
With the rise of immersive technologies such as the metaverse, users are increasingly exposed to new forms of virtual harm—such as avatar impersonation, digital harassment, and theft of virtual assets.

**Proposed actions:**

* Recognize **digital identity and virtual assets** under the law.
* Criminalize **avatar impersonation, virtual stalking, and digital property theft**.
* Develop **“virtual courts”** to resolve disputes arising in digital platforms.

**4.5 Establishment of a National Digital Resilience Council (NDRC)**

**Why it matters:**  
Cybersecurity efforts in Bangladesh are currently fragmented across different agencies and ministries. A coordinated, multidisciplinary body is essential to anticipate threats and formulate inclusive policies.

**Proposed actions:**

* Form the **NDRC** as a permanent body consisting of legal experts, technologists, ethicists, educators, and youth representatives.
* Conduct **annual reviews of cyber legislation** and oversee implementation.
* Launch **nationwide digital literacy programs**, particularly focused on youth, rural communities, and vulnerable populations.

**4.6 Regional Cyber Peace and Cooperation Framework**

**Why it matters:**  
Cyber threats often transcend borders. Regional collaboration can enhance collective response and capacity-building.

**Proposed actions:**

* Initiate a **South Asia Cybersecurity Alliance** with neighboring countries.
* Develop joint **incident response protocols**, training programs, and investigative tools.
* Position Bangladesh as a **regional hub** for ethical cyber governance and digital diplomacy.

**5. Expected Impact**

If implemented, these legal reforms will help:

* Establish a clear and enforceable digital rights regime.
* Strengthen public trust in digital platforms and government systems.
* Enhance Bangladesh’s readiness for emerging technologies.
* Foster international credibility and partnerships.
* Empower citizens through inclusive, rights-based digital governance.

**6. Implementation Plan**

| **Phase** |  |  |  | **Duration** |  |  | **Key Actions** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Research & Policy Drafting |  |  |  | 3 months |  |  | Comparative legal analysis, expert consultations |
| Stakeholder Engagement |  |  |  | 2 months |  |  | Public forums, surveys, civil society dialogue |
| Legislation Development |  |  |  | 2 months |  |  | Drafting bills, legal vetting, submission to Parliament |
| Institutional Setup |  |  |  | 3 months |  |  | Forming authorities, task forces, council formation |
| Awareness and Training |  |  |  | Ongoing |  |  | Legal education, cyber literacy, judicial training |
| Monitoring and Evaluation |  |  |  | Annual |  |  | Policy review, public reporting, legal revisions |

**7. Conclusion**

Bangladesh stands at a critical juncture in its digital evolution. Legal reforms are no longer a luxury, they are a necessity. The cyber laws of the future must be inclusive, transparent, and agile enough to adapt to rapid technological shifts.

By learning from global best practices while respecting local contexts, Bangladesh has the opportunity to create a digital ecosystem that is both resilient and empowering. Through the proposals outlined in this document, the country can lay the foundation for a secure, ethical, and forward-thinking digital future.

**8. 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] European Commission, "Proposal for a Regulation: Laying Down Harmonised Rules on Artificial Intelligence (AI Act)," European Union, 2023. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>
4.  [4] Office of the Privacy Commissioner of Canada, "Guidance on the Personal Information Protection and Electronic Documents Act (PIPEDA)," Government of Canada, 2023. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
5.  [5] CISA, "Cybersecurity Framework for Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, 2023. [Online]. Available: https://www.cisa.gov/resources-tools/resources/cybersecurity-framework
6.  [6] OECD, "Digital Government Review of Japan: Towards a Data-Driven Public Sector," OECD Publishing, 2022. [Online]. Available: https://www.oecd.org/gov/digital-government-review-of-japan-1f930fb8-en.htm
7.  [7] ARTICLE 19, "Reforming the Digital Security Act in Bangladesh: Towards a Human Rights-Based Approach," ARTICLE 19, Jan. 2023. [Online]. Available: https://www.article19.org/resources/bangladesh-reforming-the-digital-security-act/
8.  [8] Transparency International Bangladesh, "Digital Laws and Freedom of Expression in Bangladesh," TIB, 2024. [Online]. Available: https://www.ti-bangladesh.org/research/reports/2024-digital-laws
9.  [9] World Economic Forum, "Global Cybersecurity Outlook 2023," WEF, Jan. 2023. [Online]. Available: https://www.weforum.org/reports/global-cybersecurity-outlook-2023
10.  [10] BitSight, "7 Cybersecurity Frameworks to Reduce Cyber Risk," BitSight, Jul. 12, 2023. [Online]. Available: <https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk>