Assignment on

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

Submitted To
Pankaj Bhowmik
Lecturer,Department of CSE

Submitted By
Md.Anowar Hossen Labu
Student id: 2002032

Course Title:Computer Ethics and Cyber Law
Course Code :CSE 455

Department of Computer Science and Engineering
Hajee Mohammad Danesh Science and Technology University,Dinajpur

Cyber Laws in USA

Computer Fraud and Abuse Act (CFAA) of 1986

Under the CFAA, it is illegal to:

1. Access a computer without authorization.
2. Obtain financial information or government records without permission.
3. Cause damage to protected computers (e.g., viruses, ransomware).
4. Traffic in stolen passwords or access devices.
5. Use computers to commit fraud.

Penalties for Violating the CFAA:

First-Time Offense:

- Fine under U.S. federal law (amount varies by severity).
- Imprisonment for up to 5 years.
- Or both fine and imprisonment.

Repeat Offense (after previous conviction under the CFAA):

- Fine under U.S. federal law.
- Imprisonment for up to 10 years.
- Or both fine and imprisonment.

References: Computer Fraud and Abuse Act of 1986
U.S. Code: Title 18, Section 1030
https://www.congress.gov/bill/99th-congress/house-bill/4718

Cybersecurity Laws of the People's Republic of China

Cybersecurity Law Provisions and Penalties (People's Republic of China)

Article 21 states that network operators are required to establish internal security systems to protect against data leaks, cyberattacks, and other security threats. If an organization fails to comply with this requirement, they may face official warnings, orders to make corrections, and in severe cases, suspension of business operations or revocation of their licenses.

Article 22 mandates that all internet users must register with their real names before using any online services. This is meant to ensure traceability and reduce the risk of cybercrimes. Service providers that fail to enforce this rule may be penalized with service suspensions, mandatory corrections, and monetary fines.

Article 24 emphasizes that online service providers must verify the identity of users before granting access to their services. If a provider fails to do so, they may be fined up to one million RMB. In cases involving serious negligence or intentional misconduct, the responsible parties may also face criminal charges.

Article 27 strictly prohibits individuals and organizations from engaging in activities that harm cybersecurity, such as hacking, spreading malware, or unauthorized access to systems. Violators may face administrative punishment or even criminal liability, including imprisonment depending on the severity of the offense.

Articles 31 to 35 concern Critical Information Infrastructure (CII) and require operators to store personal and important data within China. Any transfer of such data outside the country must go through strict security assessments. If these rules are violated, penalties may include fines up to one million RMB, suspension of services, and even revocation of operational licenses.

Articles 41 to 43 focus on the protection of personal information. Organizations must collect personal data lawfully, with proper consent, and ensure its secure use. Mishandling personal data

can lead to large fines, mandatory compensation to affected individuals, and reputational damage through public exposure.

Articles 46 to 48 give authorities the power to summon entities or individuals for violations and demand corrective actions. If the violator refuses or fails to comply, additional and heavier penalties may be imposed, including blacklisting from future government contracts or tenders.

Article 63 clarifies that even if a violation does not qualify as a criminal offense, the individual or organization involved will still face administrative penalties. These can include warnings, confiscation of any illegal income, and monetary fines.

References:https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

Cyber laws in Germany

On 20th September 2006, the German government proposed a new draft law to fill the gaps in existing cybercrime laws. However, even before that, the German Penal Code already had several important sections related to cybercrime. Some of the key ones are discussed below:

Section 202a – Data Espionage

This law deals with illegal access to protected data. If someone collects or obtains data without proper permission, and that data was protected from public access, it is considered a punishable offense. The punishment can be up to three years in prison or a fine. This section only applies to digital data stored or transferred electronically, magnetically, or in a hidden format.

Section 303a – Alteration of Data

This section focuses on unauthorized changes to digital data. If anyone deletes, hides, damages, or changes digital data without legal permission, they can be punished with up to two years of

imprisonment or a fine. Interestingly, even attempting to do such things is also a criminal act according to this law. It helps to protect the originality and accuracy of important data.

Section 303b – Computer Sabotage

This part of the law talks about intentionally harming computer systems. If someone damages a computer or data carrier that is important for another business or government office, they can be jailed for up to five years or fined. This includes destroying systems or doing anything that disturbs important digital operations. Just trying to commit such acts is also a punishable crime.

References:https://www.upguard.com/blog/cybersecurity-laws-and-regulations-germany

Cyber Laws in South Koria

Article 141 – Invalidity of Public Documents and Destruction of Public Goods

Anyone who damages, hides, or spoils public documents or special media records (like electromagnetic records) used by government offices can be punished with imprisonment (up to 7 years) or a fine up to 10 million won.

Article 227-2 – False Preparation or Alteration of Public Electromagnetic Records

Anyone who intentionally falsifies or alters electromagnetic documents related to public officials or government offices can face imprisonment up to 10 years.

Article 232-2 – Falsification or Alteration of Private Electromagnetic Records

Anyone who falsifies or alters electromagnetic records related to private persons to cause errors in business management can be punished with imprisonment up to 5 years or a fine up to 10 million won.

Article 316 – Violation of Secrecy

Opening or reading someone else's sealed or private letters, documents, drawings, or electromagnetic records without permission can lead to imprisonment (up to 3 years) or a fine up to 5 million won. This applies also if the contents are obtained using technical means.

Article 347-2 – Fraud by Use of Computer

Anyone who gains property benefits by inputting false information or altering data in a computer or data processor without authority can be punished with imprisonment up to 10 years or a fine up to 20 million won.

Article 366 – Destruction and Damage of Property

Destroying, damaging, or hiding another person's property documents or special media records (e.g., electromagnetic records) can lead to imprisonment up to 3 years or a fine up to 7 million won.

References:https://www.kisa.or.kr/EN/301

Cyber Laws in Australia

Australian Cybercrime Act 2001 - Key Provisions and Penalties

Unauthorized Modification of Data to Cause Impairment (Section 477.2)

A person commits an offense if they intentionally modify data without permission, knowing it's unauthorized, and recklessly cause or risk impairing access, reliability, security, or operation of data on certain computers, including Commonwealth computers.

Penalty: Up to 10 years imprisonment.

Unauthorized Impairment of Electronic Communication (Section 477.3)

A person is guilty if they intentionally cause unauthorized interference with electronic communication to or from a computer, especially via telecommunications services or Commonwealth computers.

Penalty: Up to 10 years imprisonment.

Unauthorized Access or Modification of Restricted Data (Section 478.1)

If a person knowingly accesses or modifies restricted data without permission, intending to do so, especially if the data belongs to Commonwealth entities or is accessed via telecommunications services.

Penalty: Up to 2 years imprisonment.

Unauthorized Impairment of Data on Devices (Section 478.2)

A person commits an offense if they intentionally and knowingly impair the reliability, security, or operation of data on devices such as computer disks, credit cards, or other electronic storage devices owned or leased by Commonwealth entities.

Penalty: Up to 2 years imprisonment.

Possession or Control of Data with Intent to Commit a Computer Offense (Section 478.3)

Having possession or control of data with the intention that it be used to commit or facilitate an offense under Division 477, even if the offense is impossible to complete.

Penalty: Up to 3 years imprisonment.

Producing, Supplying or Obtaining Data with Intent to Commit a Computer Offense (Section 478.4)

Producing, supplying, or obtaining data with the intent to use it for committing or facilitating an offense under Division 477, regardless of whether the offense is actually committed or possible.

Penalty: Up to 3 years imprisonment.

References:https://www.homeaffairs.gov.au/cyber-security-subsite/Pages/cyber-security-act.aspx

Cyber Laws In Bangladesh

The Bangladesh Cyber Security Ordinance 2025, which supersedes the Cyber Security Act 2023, has introduced significant reforms to address cybercrimes while safeguarding citizens' rights. These changes include the decriminalization of certain offenses and the introduction of new penalties for specific cybercrimes.

Decriminalization of Defamation and Related Offenses

Previously, defamation and related offenses were non-bailable and carried severe penalties.Under the new ordinance, these offenses have been made bailable, and the maximum imprisonment has been reduced to **2 years**.Additionally, the provision for enhanced penalties in case of repeated offenses has been removed.

Criminalization of Online Abuse and Sexual Harassment

For the first time, online abuse and sexual harassment of women and children have been recognized as punishable offenses.These offenses carry a maximum imprisonment of 2 years and a fine of up to Tk 20 lakh.

Prohibition of Online Gambling

Online gambling has been banned under the new ordinance.Violations are punishable by a maximum imprisonment of 2 years and a fine of up to Tk 20 lakh.

Criminalization of Religious Hatred

The ordinance criminalizes the publication or dissemination of content that incites religious hatred.The definition of religious hatred has been clearly specified to prevent misinterpretation and misuse.

References:http://bdlaws.minlaw.gov.bd/act-1457.html

Proposed Cyber Laws in the Context of Bangladesh

Law to Combat Deepfakes and AI-Generated Fake Content

In recent times, the use of artificial intelligence to create deepfakes—manipulated images, audio, or videos—has become a growing threat. Bangladesh currently lacks a dedicated law to prevent or penalize such acts. A new legal framework should be introduced to criminalize the creation or

distribution of deepfake content with malicious intent. Offenders should face strict penalties such as imprisonment of up to 5 years and/or heavy fines.

Cybersecurity Law for Critical Infrastructure Protection

Key national infrastructure such as power grids, banks, hospitals, and transportation systems are increasingly reliant on digital systems. A specialized law is required to define and protect these sectors from cyber-attacks. Attempts to compromise such infrastructure should be categorized as acts against national security, with corresponding severe punishments.

Law Against Non-consensual Sharing of Intimate Content

In many countries like the US, UK, and India, laws criminalize the sharing of private intimate images or videos without consent, often called "revenge porn." Such acts severely harm a person's dignity and mental health. Bangladesh lacks a clear legal framework to address this, making it essential to introduce legislation that specifically punishes the unauthorized distribution of intimate content.

Law Against Fake Social Media Accounts and Identity Theft

In Bangladesh, people often create fake social media profiles using others' pictures to mislead or harm reputations. A dedicated law criminalizing the creation and misuse of fake online identities is necessary to prevent such abuses.

Cyber Financial Fraud Law

Digital financial services like bKash, Nagad, and Rocket are popular in Bangladesh, but cyber fraud related to these platforms is increasing. Unlike some countries that have clear cyber finance fraud regulations, Bangladesh still needs comprehensive legislation that targets digital payment frauds, ensuring strict penalties for offenders.