OPEN ACCESS

GRS Journal of Multidisciplinary Research and Studies

Abbriviate Tittle- GRS J Mul Res Stud

ISSN*(Online)- 3049-0561*

https://grspublisher.com/journals

V2-1,Iss-2(Feb-2025)

An Analysis from Bangladesh on the Critical Role of Cyber Law in the Protection of Users' Personally Identifiable Information

Md. Humaun Kabir[1], Dr. Aminul Islam[2], A.K.M Sohel Habib Norwroz[3], Md. Rakib Chowdhury[4], Md. Mahbub Islam[5], Mirza Md. Abu Raihan[6], Md. Nazrul Islam[7],

[1]Associate Professor, Department of Law, Sylhet International University, Bangladesh..

[2]Advocate, Supreme Court of Bangladesh, and Adjunct Assistant Professor, Law Department, Uttara University, Bangladesh.

[3]Assistant Professor, Department of Law, Sylhet International University, Bangladesh.

[4]Apprentice Lawyer, Joypurhat District Bar Association, Bangladesh.

[5]Mymensingh District Bar Association, Bangladesh.

[6]Apprentice Lawyer, Dhaka Judge Court, Bangladesh.

[7]Apprentice Lawyer, Sunamganj District Bar Association, Bangladesh.

***Corresponding Author** Md. Rakib Chowdhury

Received: 15.01.2025 **Accepted: 31.01.2025** **Published: 04.02.2025**

Abstract: Cybercrime is a multifaceted issue with extensive legal ramifications; this essay examines it from a Bangladeshi perspective. Cyber laws are necessary to protect people's rights and privacy when using the internet. This essay will delve into the various types of cybercrime, the reasons people commit them, and the significance of cybercrime laws. This study derives some conclusions after reviewing the anti-cybercrime laws that Bangladesh has already passed. Several pieces of legislation are housed here, including those that deal with IT, PC, CS, and the Bangladesh Telecommunication Regulatory Commission (TROC)2001.

Not only does the study consider these specific restrictions in its comprehensive legal analysis, but it also takes into consideration more general rules, including the Copyright Act of 2005, the Constitution of the People's Republic of Bangladesh, and the Bangladesh Penal Code of 1860. As case studies, the article includes notable cybercrime instances in Bangladesh. We can observe the impact of judicial rulings on national cybercrime control initiatives in these cases. The article continues by outlining the difficulties faced by the government of Bangladesh in its fight against cybercrime and for the safe use of the internet by its inhabitants.

Keywords *Cybercrime, Cyber laws in Bangladesh, Privacy protection, Anti-cybercrime legislation, Internet rights, Bangladesh Penal Code, Bangladesh Telecommunication Regulatory Commission, Copyright Act, Judicial impact on cybercrime, Government challenges in cybersecurity.*

Introduction

An integral part of modern life, the internet has revolutionized digital communication, work, and interaction all around the globe. More and more people are putting their trust in internet platforms and disclosing extensive personal details. This highlights the critical need of safeguarding personal information. Critical in addressing this issue, cyber laws provide norms and legal frameworks for regulating internet use and ensuring the security of sensitive data.

Cyber laws in Bangladesh are extremely important since they protect people's privacy when they use the internet. The Digital Security Act of 2018 is a crucial piece of legislation in the battle against cybercrimes and in protecting people's privacy. It creates rules on the use of personal data and penalties for violations of these rules. To combat the growing threats posed by cybercrime and other technological advancements, it is essential to implement these measures to safeguard the privacy of internet users. These regulations need frequent updates to ensure the continued security of digital environments and their ability to accommodate emerging technologies (Kamal, 2020; Rahman, 2021).

Literature Review

1. Overview of Cybercrime and Privacy Concerns:

The rise of cybercrime in the modern era has been a major concern for governments, companies, and individuals around the globe. The potential for breaches of Personally Identifiable Information (PII) grows in tandem with the expansion of internet usage. According to research, strong legislative frameworks are necessary to guarantee users' privacy, which is a basic human right (Kamal, 2020). Identity fraud, cyber stalking, unauthorized data access, and online fraud are all crimes that cyber laws aim to combat. In addition, they give penalties for infractions and lay up standards for managing technical vulnerabilities (Rahman, 2021).

2. Cyber Laws in Bangladesh:

Two of the most important pieces of legislation in Bangladesh's

***Corresponding Author:** Md. Rakib Chowdhury

legal framework pertaining to cybercrime are the Digital Security Act of 2018 and the Information and Communication Technology (ICT) Act of 2006. There are still loopholes in these regulations that don't adequately handle the ever-changing cyber risks. One example is the ICT Act, which has drawn criticism for its harsh and nebulous punishments and for its narrow coverage of cyber offenses (Rahman & Karim, 2019).

While the Digital Security Act is more recent, some worry that it could be abused and doesn't adequately protect personal information. To remove gaps and bring it in line with international privacy protection norms, this law has to be amended (Ahmed, 2021). Research of foreign frameworks suggests that GDPR, the EU's General Data Protection Regulation, might be used as a model for better cyber legislation in Bangladesh.

3. Challenges in the Implementation of Cyber Laws:

There are a lot of obstacles to enforcing cyber laws in Bangladesh, such as a shortage of trained police officers and an outdated network infrastructure. The government is also unable to respond adequately to cyber attacks because no dedicated agency deals with this type of crime (Ahmed, 2021). The fight against cybercrime is already complicated, and judicial interpretations of current rules frequently reveal legislative gaps.
Problems with public awareness have also been found in the research. There are legal channels for reporting cybercrimes, but many people do not know about them or their rights. People are more susceptible to exploitation, and current regulations are less effective due to this lack of understanding (Kamal, 2020).

4. International Comparisons:

When compared to other countries' cyber laws, Bangladesh's are significantly weaker when it comes to protecting personal information and data. Comprehensive cyber security policies combining legislative measures with technology innovation have been established by countries like Estonia and Singapore (Rahman, 2021). These cases show that Bangladesh has to take a broader view that includes regulatory and technical fixes.

5. Judicial Impact and Notable Cases:

The implementation of cyber laws in Bangladesh has been greatly influenced by judicial rulings. More exact legal definitions and harsher punishments for violators have been brought to light by notable cases. Consider how data breach case verdicts have shown where the ICT Act is lacking and how court interpretations differ from legislative purpose (Rahman & Karim, 2019).

6. Policy Gaps and Recommendations:

Legislative and regulatory frameworks addressing cybercrime in Bangladesh still have a long way to go, despite advances. Problems such as inadequate punishments for cybercrimes, a lack of procedures to align local legislation with international norms, and the absence of an institution specifically charged with preventing cybercrime are crucial (Ahmed, 2021).
Several academics have proposed filling these holes by creating a dedicated cybercrime unit, revising current laws to better deal with cybercrime, and drafting new laws to deal with new types of cybercrime. For example, according to Kamal (2020), cybercrime crimes may be tried more fairly if separate cyber tribunals were established.

Methodology

By reviewing existing legal frameworks, case studies, and secondary data sources, this qualitative study seeks to understand how cyber laws in Bangladesh safeguard users' personal information. The research was grounded in a thorough review of key legal documents, including the following: the Information and Communication Technology (ICT) Act of 2006, the Digital Security Act of 2018, the Pornography Control Act of 2012, the Copyright Act of 2005, the Bangladesh Telecommunication Act of 2001, the Bangladesh Penal Code of 1860, and the Bangladesh Telecommunication Act of 2001. These legislative texts were reviewed for particular provisions, enforcement methods, and gaps pertaining to cybercrime and privacy protection.

Looking at notable cybercrime occurrences that happened in Bangladesh helped put these restrictions into perspective. These cases provided valuable insight into judicial interpretations and shed light on the challenges faced by regulatory and law enforcement organizations in their fight against cybercrimes. We supplemented primary research with secondary sources, such as official documents, academic studies, and expert opinions, to ensure a thorough understanding of the issues. Academics like Rahman (2021) and Kamal (2020) did a lot to help with both theory and practice.
Cyber rules in Bangladesh were compared to those in other nations as part of the research's comparative approach. Because of this, we were able to identify areas where national laws may be improved by aligning with global frameworks so that they are more in accordance with international standards. This thorough assessment uncovered numerous policy gaps and difficulties, including insufficient enforcement procedures, the absence of a designated cybercrime agency, and the deficiencies of the ICT Act of 2006.

Concrete recommendations for enhancing the legislative and regulatory climate were subsequently derived from the findings of these assessments. It is imperative to create a specialized organization to combat cybercrime, update existing legislation, and align local cyber laws with international norms. This all-encompassing methodology ensures a comprehensive evaluation of the critical role of cyber laws in protecting users' personal information in Bangladesh by filling in the gaps and solving the difficulties in the present legal framework.

Specify the Issue at Hand

There has been a concerning rise in the amount of cybercrime that has occurred in the modern digital age, and one of the reasons for this is the widespread usage of gadgets that are connected to the internet. Because of its many facets, cybercrime affects a large number of people all over the world. A great number of individuals experience mental, emotional, and financial losses as a direct result of cybercrime. Despite the fact that adults and children are both unfairly targeted, the data indicate that the kids of today are especially susceptible to being negatively affected. This group is confronted with a number of challenges, including easy access to illegal substances, exposure to pornographic websites, and theft of personal information. Although some of these young individuals go on to commit crimes, a significant number of them develop an interest in criminal activity as a result of viewing content of this nature. Because cybercrime has an effect not only on individuals but also on society as a whole, it is of the utmost importance to find solutions to the problem and to put safeguards in place to

prevent it.

The Crime of Cyber

Cybercrime, which encompasses a wide range of illicit activities conducted in the digital realm, poses a significant threat to Bangladesh. There are many types of cybercrime in the country, including cyber bullying, fraud, hacking, identity theft, and the distribution of damaging content. Stricter laws are needed to deter thieves and safeguard vital infrastructure due to the rise in frequency and severity of these crimes, which have been exacerbated by the widespread use of social media and online financial services. Bangladeshi lawmakers have recognized cybercrime as a serious issue and have enacted measures to combat it (Ahmed & Rahman, 2021).

Even with these regulations in place, cybercrime continues to be a concern for individuals, businesses, and government institutions. While it's encouraging that law enforcement has cybercrime teams, it's important to remember that laws and enforcement strategies must adapt to keep up with the dynamic nature of digital technology (Khan, 2020). Without these improvements, combating Cybercrime and ensuring public safety in the digital age will be challenging.

Reasons for cybercrime in Bangladesh

Cybercrime in Bangladesh is a growing concern, driven by various factors that stem from social, economic, and technological dynamics. These factors contribute to an environment where cybercriminals can exploit vulnerabilities. Below are the primary reasons why cybercrime occurs in Bangladesh:

1. **Rapid Digitalization with Limited Cybersecurity Awareness:**

- **Rapid Digitalization:** Bangladesh has witnessed significant advancements in digital infrastructure over the past decade. The proliferation of mobile banking, e-commerce, social media, and digital communication has created vast opportunities for cybercriminals to exploit.
- **Lack of Awareness:** Many users lack basic knowledge of cybersecurity practices, such as using strong passwords, avoiding phishing scams, or securing personal data. This makes individuals and businesses easy targets for cybercriminals.
- **Digital Literacy Gap**: While the government has promoted digital literacy, many citizens, especially in rural areas, are unfamiliar with safe online practices, leaving them vulnerable to scams and fraudulent activities.

2. **Inadequate Legal Framework and Enforcement:**

- **Insufficient Laws:** Though Bangladesh has laws such as the Digital Security Act, 2018, the legislation often lacks specificity or adaptability to address the rapidly evolving nature of cybercrime.
- **Weak Enforcement:** Law enforcement agencies often face challenges in tracking and prosecuting cybercriminals due to insufficient training and limited technical resources.
- **Jurisdictional Issues**: Cybercrimes often involve international networks, which complicates investigation and prosecution due to jurisdictional limitations and lack of international cooperation.

3. **Economic Motivations:**

- **High Unemployment and Poverty**: A significant portion of the population faces economic hardship, leading some to engage in cybercrime as a means of financial gain.
- **Low Cost of Entry:** Unlike traditional crimes, cybercrime often requires minimal resources, such as a computer and internet connection, making it accessible to individuals seeking quick financial benefits.

4. **Technological Advancements and Increased Connectivity:**

- **Rise of Smart Phones and Internet Use:** The widespread adoption of smart phones and affordable internet access has exponentially increased the number of internet users in Bangladesh, providing cybercriminals with a larger pool of potential victims.
- **Weak Security Systems:** Many organizations and individuals fail to implement robust security measures, such as firewalls, encryption, and secure networks, making them vulnerable to hacking and data breaches.

5. **Social Factors and Cultural Norms:**

- **Lack of Ethical Awareness**: Many individuals do not fully understand the ethical implications of their online actions, such as hacking or spreading misinformation.
- **Cyber Harassment and Gender Issues**: Women are disproportionately targeted in cyber harassment cases due to cultural stigmas, creating a toxic online environment and perpetuating gender-based cybercrimes.
- **Social Engineering**: Cybercriminals often exploit trust-based relationships through scams or phishing attempts, leveraging the victim's lack of caution or awareness.

6. **Inadequate Cyber Security Infrastructure:**

- **Limited Investment in Cyber Security**: Many organizations, especially small and medium enterprises (SMEs), do not prioritize cyber security due to cost concerns or lack of awareness about its importance.
- **Shortage of Skilled Professionals**: Bangladesh faces a shortage of cyber security experts, leaving critical infrastructure and sensitive information vulnerable to attacks.

7. **Global Influence and Exposure:**

- **International Cybercrime Syndicates**: Global cybercriminal networks often target Bangladesh due to perceived weaknesses in its cyber security infrastructure.
- **Cross-Border Crimes**: The interconnected nature of the internet enables criminals from other countries to exploit Bangladesh's vulnerabilities without being physically present.

8. **Emerging Technologies and Trends:**

- **Cryptocurrency:** The rise of cryptocurrencies have made it easier for cybercriminals to launder money or demand ransom in ransomware attacks.
- **Dark Web:** The availability of illegal tools and resources on the dark web enables individuals to engage

in cybercrime without significant technical expertise.

Guaranteed rights in the context of cyberspace

1. Equal Access to Diverse Media:

Anyone with an internet connection should be allowed to see any kind of media they want. By increasing awareness of the risks posed by industry consolidations, the open Internet is protected. Abuse of market dominance through M&As can reduce competition in other sectors (Napoli, 2019). Netizens' (those who use the internet) rights centred on four principles: privacy, access to information, digital freedom, and protection from harm in the digital realm (MacKinnon, 2012). Ongoing vigilance from governments and users is essential for a media environment that is both free and diversified.

2. The Right to Free Speech:

Internet users should not be subject to excessive restrictions or threats of retaliation for expressing their opinions and ideas online. By virtue of Article 19 of the UDHR, all people are assured the right to exist, to be free, and to pursue happiness (United Nations, 1948). The right to freely express and receive ideas, as well as unrestricted access to information across borders and media are guaranteed by it (OHCHR, 2018). The promotion of free speech and innovative ideas in online communities relies heavily on this autonomy (La Rue, 2011).

3. Preserving Data and Ensuring Confidentiality:

A person has the right to privacy if they want to be able to manage their own data, keep their correspondence private and not have their personal space violated. An individual's right to privacy was guaranteed in 1966 by the United Nations through the International Covenant on Civil and Political Rights (ICCPR). Strict legislative frameworks are necessary to guarantee data privacy in the digital era due to technological improvements (Greenleaf, 2014).

4. Information Availability:

The right to access publicly available information should not be restricted to any entity, including governments or enterprises. The right to know is a fundamental human right. says the United Nations Human Rights Council (UNHRC, 2016). This right is a component of freedom of expression, as both the UDHR and the ICCPR make clear in Article 19. The United Nations Human Rights Council has, in its reports and resolutions, emphasized the importance of information access on multiple occasions, reflecting its efforts to combat censorship and promote openness (UNESCO, 2015).

a) **Universal Declaration of Human Rights (UDHR):** Article 19 of the UDHR defines access to information as a component of freedom of expression, ensuring every individual's right to seek, receive, and share information (United Nations, 1948).
b) **International Covenant on Civil and Political Rights (ICCPR):** The ICCPR reinforces the right to information access, mirroring Article 19 of the UDHR (United Nations, 1966).
c) **UNHRC Reports and Resolutions:** The UNHRC regularly emphasises the significance of information access and advocates for the removal of barriers to free expression (UNHRC, 2016).

5. Liberty of the Press:

Bangladesh's Constitution of 1972 guarantees the fundamental liberties of freedom of speech and expression, as well as freedom of the press. However, these liberties may be subject to reasonable restrictions, which can create practical challenges (Rahman, 2020). In order to ensure the dissemination of impartial and diverse viewpoints, it is essential to maintain press freedom.

6. Equal Access to Cyber Protection:

People are beginning to understand the crucial importance of digital security on a global scale. According to UNESCO's 2015 report, cyber security and digital rights have been designated as major priorities by the UN, the ITU, and other international organisations. More than a hundred nations have the opportunity to hone their reaction and management skills through the International Telecommunication Union's (ITU) cyber drills (ITU, 2020). The increasing significance of safeguarding digital environments for all users is highlighted by these programs (Floridi, 2014).

7. Protection of Intellectual Property and Authorship:

The fundamental goal of copyright laws is to guarantee that people who initially created works of art, literature, or music may keep making money off of their hard work. The public at large must be careful and get the proper permissions before using these rights, with a few exceptions, including fair use and public domain licenses (Lessig, 2008). In an effort to foster equal access and protect writers' intellectual property, the Constitution of 1972 of Bangladesh ensures that all citizens have copyright and fair use. rights. When people may claim ownership of their own works in the metaverse and other online venues, these rights become even more important (Van Dijk, 2020).

The Authority Over Cyber Space in Bangladesh

The complex and ever-changing nature of the internet legislation is reflected in Bangladesh's cyber jurisdiction. The authority of a court to decide on disputes or accept cases that have been formally presented for examination is referred to as "governance" in this context (Warren & Brandeis, 1890). Questions of jurisdiction about the applicability and enforceability of territorial laws in the digital age have emerged in light of the internet's ever-expanding reach and impact outside traditional national boundaries. For instance, according to Bazelon (2020), governments are finding it harder to draw distinct boundaries between their control over online behaviour and the laws that govern it due to the expansion of the internet. The capacity of governments to regulate worldwide digital platforms and the relevance of existing legal frameworks to transnational activity has emerged as a concern in the wake of the Internet's rapid expansion (Cameron, 2019). For instance, the Information & Communication Technology Act, 2006, a crucial statute in Bangladesh, applies to any crime committed on computer systems or networks within the country, notwithstanding the location of the crime (Bangladesh Ministry of Statute, 2006).

Section 4 of the Information and Communication Technology (ICT) Act of 2006, as reported by the Bangladesh Ministry of Law

(2006), gives the Bangladeshi courts the power to consider cases involving cybercrimes related to the nation, whatever the location of the offence. As per the Bangladesh Law Commission (2005), it is guaranteed that crimes committed by Bangladeshi people can be tried under Bangladeshi law no matter where they are, according to Section 4 of the Penal Code of 1860. According to the Bangladesh Ministry of Law (2015), the concept of geographical jurisdiction was established in the Code of Criminal Procedure, 1898, which means that courts in Bangladesh can handle cases involving its citizens regardless of the location of the offence.

Multiple Measures to Ensure the Safety of Neighbours Online

1. The Information and Communication Technology Act, 2006:

With the passage of the Information and Communication Technology Act, 2006 (ICT Act), Bangladesh fortified its legal framework pertaining to information technology and aimed to reduce the prevalence of cybercrimes. The Act's stated purpose was to formally acknowledge and safeguard the nation's IT systems. In an effort to curb and penalise illegal activities such as hacking, cyber bullying, and identity theft that take place on the internet, the law established sanctions for individuals who disobeyed its rules. The Act has undergone several revisions over the years to better address new technologies and online crimes and to keep up with the constantly evolving cyber risks. (Islam & Ahmed, 2019).

2. The Digital Security Act, 2018:

In addition to the ICT Act, the Digital Security Act of 2018 further restricted the dissemination of false information, rumours, hate speech and defamation on the internet. The proliferation of cybercrimes is directly attributable to the act. It is the purpose of the act to limit the ability of online platforms to spread terrorist, racist, extremist, and sectarian content. Another perk is the power to punish people who spread offensive, nasty, or otherwise inappropriate content. Nevertheless, the bill's broad and nebulous language has ignited heated debate, as many are worried about its potential use to censor free expression. The assumption that the The Digital Security Act is being used to censor dissenting opinions, which has led to the incarceration of journalists, activists, and critics of the government. The Cyber Security Act, an updated version of this law that aimed to strengthen internet governance and security, was passed in 2023 (Chowdhury, 2021).

3. The Copyright Act, 2005:

Following its changes to the Copyright Act of 2000, the The Copyright (Amendment) Act, 2005, replaced the Copyright Ordinance of 1962. May 18, 2005 was the date of its passing. Dealing with copyright issues related to digital media, this act aims to protect intellectual property in the digital age. Notably, the modification retains the ability to provide proof of ownership in case of a disagreement while making copyright registration optional. The legislation conforms to international agreements such as the TRIPS Agreement and the Berne Convention to ensure that copyright protections are acknowledged worldwide. Producers and consumers are safeguarded against legal action in the case of violation by including programming languages, digital databases, multimedia assets, and performers' rights (Rahman, 2020).

Attacks on Bangladeshi Cyberspace

In today's world, when communication technologies are Converging at a rapid pace, the internet has become increasingly vital. The proliferation of online shopping, banking, ticket purchasing, and lottery participation, data transfer, and bidding have created several opportunities, but it has also exposed individuals to significant risks (Ahmed, 2019). Cyber Fraud is a real threat in our digital world; therefore, we must be careful. The The Information and Communication Technology Act of 2006 of Bangladesh does not provide a precise definition of cyber fraud (Ahmed, 2019), but it does include many provisions to control and avoid the crime. Data storage devices (such as CDs, floppy discs, and DVDs), databases, and computers are all targets of the law's felony division when stolen. Anyone caught accessing, copying, downloading, or extracting material without authority, faces severe penalties, including prison terms of seven to fourteen years, according to the law (Ahmed, 2019). The offender may also be subject to a reparation fine of up to one crore. Taka (Ahmed, 2019). Bangladesh is taking these measures to safeguard its citizens in the digital age and prevent cyber fraud.

An Analysis of the Cyber Vault Incident in Bangladesh

In 2016, a group of hackers launched a sophisticated cyber attack against the central bank of Bangladesh, attempting to steal around $1 billion from the bank's account at the Federal Reserve Bank of New York. Through malware, the hackers were able to access the bank's SWIFT network. which handles international money transfers. However, despite the government's best efforts, a grand amount of $81 million was sent to various accounts in the Philippines (Haque, 2019). Even though part of the stolen funds were eventually recovered, the incident nevertheless caused worldwide investigations and highlighted the flaws in the global banking system. Following extensive investigations into their responsibilities in the heist, an eight-person jury in Bangladesh carried out the execution of a former bank employee and numerous IT technicians in 2019 (Hossain, 2020).

In 2011, a lady called Rumana Manzur—of mixed Bangladeshi and Canadian heritage—was brutally attacked via cybercrime and domestic violence. Hasan Sayeed Sumon, her husband, viciously assaulted her after suspecting her of infidelity due to her social media activity. He ripped out her eyeballs and inflicted other severe injuries (Ahmed, 2013). This tragic event highlighted the potential dangers of online interactions and the necessity for stronger legal protections for victims of cyber bullying and domestic abuse (Jahan, 2014). After Sumon was found guilty and given a life sentence in 2013 for the horrific attack on his wife, debate started about the need to address cybercrime and domestic violence within legal frameworks (Sarkar, 2015).

Want to Argue About a Ransomware Attack (2017)

In May 2017, a global ransomware attack known as Wanna Cry happened, and it affected Windows PCs. Aiming to encrypt user data and demand Bitcoin as ransom to decode it, this cyberattack launched. Server Message Block (SMB), Windows' file-sharing protocol, has a security hole that Wanna Cry exploited (Symantec, 2017). Users neglected to update their software, leaving many machines vulnerable to attackers who exploited the weakness in older versions of Windows, even though Microsoft issued a fix for

the flaw months ago (Kaspersky, 2017).

The attack affected over 150 nations and over 200,000 machines; noteworthy victims included the Spanish telecoms giant Telefonica, the United Kingdom's National Health Service (NHS), and FedEx (Symantec, 2017). The hackers demanded Bitcoin payment within a certain timeframe, or else they would permanently delete all encrypted data from their locked computers. None of these companies were immune to the widespread upheaval that followed (Fruhlinger, 2017).

Lazarus Group, a notorious North Korean cybercrime ring, is responsible for Wanna Cry and other high-profile cyberattacks (Kaspersky, 2017). The incident highlighted the significance of maintaining solid cybersecurity practices, such as creating secure data backups and regularly updating software, to mitigate the effects of attacks like these. Cyberattacks are on the rise, and this incident highlights the need for international cooperation to safeguard critical infrastructure (Symantec, 2017).

Exploring the Difficulties of Cyber Law

The challenges associated with cyber law enforcement in Bangladesh are multifaceted, stemming from limitations in technology, legal frameworks, and human resource capacity. Below is a detailed analysis of these challenges with appropriate references.

1. Accessing Electronic Evidence: Accessing electronic evidence remains one of the most significant challenges. Despite legal provisions allowing law enforcement agencies to compel service Despite the willingness of service providers to cooperate, implementation remains weak due to officials' lack of awareness regarding their authority (Hossain, 2022). Furthermore, service providers often resist compliance, citing privacy concerns or jurisdictional issues, which delays investigations.

2. Complexity of Evidence Collection: Collecting evidence in cyber-related cases involves a complicated process. This process becomes particularly complex when tracing the origin of cyber attacks or crimes. Examples include online harassment targeting young women and cases where competitors sabotage businesses through malicious online activities. Identifying the origin of these activities is particularly difficult when the information is hosted abroad. In such cases, investigators must rely on mutual legal assistance. treaties (MLATs), which add another layer of complexity and time delays (Rahman & Akhtar, 2021).

3. Improper Handling of Electronic Evidence: Many investigators lack the expertise required to handle electronic evidence. according to established admissibility guidelines. Consequently, critical evidence is often rejected by courts. For instance, improperly extracted or stored digital evidence frequently leads to case dismissals (Kabir, 2023).

4. Chain of Custody Issues: Ensuring the proper chain of custody for electronic evidence is crucial for its admissibility in court. The transfer of evidence between institutions often results in mishandling or loss of integrity, which jeopardises prosecutions (Ahmed, 2022).

5. Insufficient Digital Forensics Infrastructure: Law enforcement agencies in Bangladesh lack sufficient resources and advanced digital forensic tools. In many cases, investigators must rely on private cyber forensic firms, which can be costly and time-consuming. This is particularly problematic in cases of cybercrimes such as bank frauds, where international cooperation is required (Chowdhury, 2023).

6. Delays in Evidence Collection: The process of evidence collection is often delayed, especially in cases involving cross-border cybercrimes. For instance, internet banking fraud frequently originates from external sources, necessitating cooperation from foreign authorities. This reliance on international collaboration prolongs investigations and prosecutions (Islam, 2024).

7. Lack of Skilled Personnel: Bangladesh faces a shortage of trained professionals capable of addressing the growing complexities of cyberspace. Many law enforcement personnel lack technical expertise, making it difficult to combat sophisticated cybercrimes effectively. This gap is exacerbated by the continuous evolution of hacking. techniques. (Sultana & Rahman, 2022).

8. Rise in Cyber-Terrorism and Lack of Awareness: The proliferation of online resources related to hacking and cybercrime has enabled cybercriminals to become increasingly skilled. Simultaneously, societal awareness about the risks of cyberattacks remains low, further compounding the issue (Ali, 2021).

9. Limited Knowledge Within Cyber Cells: The technical proficiency within Bangladesh's cybercrime units is minimal. Many officials in these units lack the digital literacy needed to keep up with young, tech-savvy hackers, making it difficult to identify and apprehend cybercriminals (Haque, 2023).

10. Inadequate Government Budget: The budget allocated for cyber law enforcement and training programs is insufficient compared to the growing need for cybersecurity measures. This financial limitation prevents the government from equipping cyber cells with the latest tools and technologies (Khan, 2024).

11. Loopholes in Existing Cyber Laws: The current legal framework for cybercrime in Bangladesh is not exhaustive and contains significant loopholes. To address the challenges effectively, these laws must be standardised to align with global best practices. Additionally, stricter regulations and public awareness campaigns are required to enhance cybersecurity measures (Rahim, 2023).

12. Global Perspective Standardisation: Cyber laws in Bangladesh need to be updated and standardised to reflect international perspectives. For instance, enhancing national privacy and adopting global data protection standards is essential for improving cyber laws and securing citizens' digital lives (Faruk, 2023).

Findings

The study identified several keys. issues regarding the legislative framework for addressing cybercrime in Bangladesh:

1. Experts deem the Information and Communication Technology (ICT) Act of 2006 inadequate to comprehensively address cybercrime in the country. Only a limited number of its provisions deal with cybercrime, and even those lack clarity and specificity (Rahman & Karim, 2019).

2. The ICT Act of 2006 imposes punishments that are often misaligned with the severity or nature of the cyber offences, raising concerns about its practical applicability.
3. While the Pornography Control Act of 2012 and The provisions against child pornography aim to combat its spread. explicit content online, these measures do not entirely cover the broad spectrum of cybercrime. The enforcement mechanism under this act remains insufficient, as the root causes of distributing pornographic content via the internet are inadequately addressed (Ahmed, 2021).
4. Cybercrime is notably absent in the Bangladesh Penal Code, although Section 13 outlines offenses that are somewhat related to cyber-related misconduct.
5. The Bangladesh Telecommunication Act of 2001 primarily regulates cellular networks and telecommunications but lacks relevance to modern cybercrime, as it neither incorporates contemporary digital crimes nor reflects recent technological advancements.

Recommendations

1. **Establishment of a Specialized Cyber-Crime Protection Agency:**
   To effectively combat cybercrime, the government of Bangladesh should establish a dedicated agency named the "Cyber Crime Protection Unit" (CCPU) under the Ministry of Home Affairs. The headquarters of the CCPU will be located in Dhaka, with the Director General (DG) serving as its head. The agency's key functions would include ensuring the safety of netizens, apprehending cybercriminals, enforcing cyber-related laws, raising public awareness, and implementing preventive measures to curb cybercrime.
   - The CCPU would operate similarly to the Rapid Action Battalion (RAB) but focus exclusively on cyber-related offenses.
   - The agency will be structured to include eight zones corresponding to the eight divisions of Bangladesh (e.g., CCPU-1, CCPU-2). Each zone will further have sub-zones at the district level, ensuring coverage from urban centers to rural areas.
   - Officers of this unit, starting from the rank of Assistant Sub-Inspector (ASI), will have the authority to investigate, arrest, and take necessary legal actions against cybercriminals.
   - The establishment of the CCPU will significantly contribute to building a "SMART" Bangladesh by enhancing cyber security and fostering public confidence in digital safety.
2. **Amendment and Implementation of the ICT Act 2006:**
   Immediate steps must be taken to address and rectify the flaws in the ICT Act 2006. Following these amendments, the revised act should be uniformly implemented across the entire country to ensure its effectiveness in combating cybercrime.
3. **Strengthening and Updating Cyber Laws:**
   Existing laws related to cybercrime should be strengthened through amendments, and new legislation should be introduced to address the evolving landscape of cyber threats.
   - Developing these laws requires the active involvement of legal experts, policymakers, and other stakeholders.
   - New enforcement mechanisms should accompany these laws to ensure robust implementation and better protection against cyber threats.
4. **Exemplary Punishments for Cyber-Criminals:**
   Stringent and exemplary punishments should be introduced and enforced for cybercriminals. This will act as a deterrent, reducing the likelihood of future offenses and enhancing the safety of individuals and organizations against online threats. Collaborating with legal authorities is essential to ensure that criminals are held accountable for their actions.
5. **Independence of Cyber Tribunals:**
   To ensure fairness and impartiality in the trial of cybercrime cases, the independence of Cyber Tribunals must be guaranteed. These tribunals should be empowered to operate without external influence, strictly following the jurisdiction provided under cyber laws. Independent tribunals can significantly enhance the suppression of cyber-crime in Bangladesh.
6. **Harmonizing Cyber Laws with International Standards:**
   Cyber laws in Bangladesh should align with international human rights laws to protect individuals from violations. Developing these laws in accordance with global standards will ensure their effectiveness while maintaining consistency with international legal frameworks.
7. **Development Through National and Legal Mechanisms:**
   The government should utilize national laws and various implementation mechanisms to continuously develop cyber laws. This approach will help address the challenges posed by the rapidly changing cyber environment and ensure the sustainability of legal frameworks for cyber security.

Conclusion

By filling in the gaps in cyber laws and making sure they are fully implemented, the government of Bangladesh can effectively combat cybercrime. To effectively combat cybercrime, it is necessary to fortify these regulations and address their shortcomings. To make these legal measures as effective as possible, it is crucial that government and law enforcement authorities work together properly.

Protecting individuals' privacy online has become more important in the modern day, and cyber legislation is a key component in this effort. Cyber laws aid in the prevention of data breaches, regulation of surveillance methods, and security of personal information by setting defined limits and imposing penalties for infractions. In addition to bolstering public confidence in the digital environment, these steps safeguard the basic right to privacy. In the end, people will be able to confidently navigate the digital world thanks to thorough and strictly implemented cyber regulations, which make

the internet a safer place.

References

1. Kamal, S. (2020). *Cybersecurity and digital privacy: Challenges in Bangladesh*. Journal of Digital Security, 5(3), 45–59.
2. Rahman, A. (2021). The role of the Digital Security Act in addressing cybercrimes in Bangladesh. International Review of Law and Technology, 8(1), 78–90.
3. Ahmed, S. (2021). Cybercrime and its legal implications in Bangladesh: A critical analysis. Dhaka Law Review,15(2), 45–60.
4. Kamal, M. (2020). The role of legislation in Ensuring digital privacy: Lessons for Bangladesh. Bangladesh Journal of Legal Studies, 22(3), 78–91.
5. Rahman, M. H. (2021). Comparative analysis of data protection laws: The case of Bangladesh and the EU. International Journal of Cyber Law, 19(4), 312–340.
6. Ahmed, S., & Rahman, M. (2021). Cybersecurity challenges in developing countries: The case of
7. Bangladesh. Journal of Cyber Crime Studies, 15(3), 200–215.
8. Khan, T. (2020). Strengthening cybercrime laws in Bangladesh: A critical analysis of current frameworks. Bangladesh Law Review, 22(4), 120–135.
9. Constitution of Bangladesh. (1972). The People's Republic of Bangladesh.
10. Floridi, L. (2014). The Onlife Manifesto: Being Human in a Hyperconnected Era. Springer.
11. Greenleaf, G. (2014). Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford University Press.
12. International Telecommunication Union (ITU). (2020). Global Cybersecurity Index.
13. La Rue, F. (2011). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. United Nations.
14. Lessig, L. (2008). Remix: Making Art and Commerce Thrive in the Hybrid Economy. Penguin.
15. MacKinnon, R. (2012). Consent of the Networked: The Worldwide Struggle for Internet Freedom. Basic Books.
16. Napoli, P. M. (2019). Social Media and the Public Interest: Media Regulation in the Disinformation Age. Columbia University Press.
17. OHCHR. (2018). Universal Declaration of Human Rights. United Nations
18. Rahman, S. (2020). Freedom of Press in Bangladesh: Challenges and Prospects. Asian Journal of Social Sciences, 18(4), 23-34.
19. United Nations. (1948). Universal Declaration of Human Rights.
20. United Nations. (1966). International Covenant on Civil and Political Rights.
21. UNHRC. (2016). Resolution on the Promotion, Protection, and Enjoyment of Human Rights on the Internet.
22. UNESCO. (2015). Keystones to Foster Inclusive Knowledge Societies.
23. Van Dijk, J. (2020). The Digital Divide. Polity Press.
24. UNESCO. (2015). Press Freedom and Sustainable Development.
25. ITU. (2020). Cybersecurity Capacity Building.
26. United Nations Human Rights Council (UNHRC). (2016). Access to Information as a Human Right.
27. Bazelon, E. (2020). Cyberspace and governance: The challenges of cross-border laws. Global Governance Press.
28. Bangladesh Law Commission. (2005). The Penal Code of Bangladesh. Dhaka: Government of Bangladesh.
29. Bangladesh Ministry of Law. (2006). Information & Communication Technology Act, 2006. Dhaka: Government of Bangladesh.
30. Cameron, D. (2019). Global challenges of cyber jurisdiction and cross-border governance. Journal of Internet Law, 23(4), 45-60.
31. Chowdhury, A. (2021). The Digital Security Act, 2018: A critical assessment. Journal of Bangladesh Legal Studies, 34(2), 78-92.
32. Hossain, M., & Rahman, M. (2020). Copyright laws in Bangladesh: A comprehensive analysis of the 2005 amendments. International Journal of Law and Technology, 5(1), 22-35.
33. Islam, S. M., & Ahmed, N. (2019). Cybercrime and legal frameworks in Bangladesh: A review of ICT Act, 2006. South Asian Journal of Law, 8(3), 45-59.
34. Sarker, M. A. (2022). The role of the Cyber Security Act in shaping digital discourse in Bangladesh. Bangladesh Journal of Cyber Law, 14(1), 112-130.
35. Ahmed, A. (2019). Cyber fraud and its legal implications in Bangladesh: An analysis of the ICT Act, 2006. International Journal of Cyber Security, 4(2), 51-66. https://doi.org/10.1234/ijcs.2019.0205
36. Ahmed, A. (2013). Cyberbullying and domestic violence in Bangladesh: A case study of Rumana Manzur. South Asian Journal of Law and Society, 7(2), 145 16Haque, S. (2019). The Bangladesh cyber heist: A case of financial vulnerability and international security. Journal of Cybersecurity and International Law, 14(4), 218-230.
37. Hossain, M. (2020). Bangladesh cyber heist: Investigations and judicial outcomes. International Journal of Financial Cybercrime, 12(3), 77-89.
38. Jahan, N. (2014). Social media, cyberbullying, and domestic violence in Bangladesh. Gender and Technology Journal, 5(1), 82-98.
39. Sarkar, R. (2015). Legal frameworks for combating cybercrime and domestic violence in Bangladesh. Asian Legal Review, 9(1), 32-49.
40. Fruhlinger, J. (2017). What is WannaCry ransomware and how does it work? CSO Online. Retrieved from https://www.csoonline.com/article/3197020
41. Kaspersky. (2017). WannaCry ransomware attack: What we know. Kaspersky. Retrieved from https://www.kaspersky.com
42. Symantec. (2017). Wanna Cry ransomware attack. Symantec. Retrieved from https://www.symantec.com.
43. Ahmed, S. (2022). Challenges of digital evidence management in Bangladesh. Dhaka: University Press.
44. Ali, M. (2021). Cyberterrorism and societal awareness in South Asia. Chittagong: Cybersecurity Journal.
45. Chowdhury, T. (2023). Digital forensics: Issues and advancements in Bangladesh. Sylhet: ICT Innovations.
46. Faruk, A. (2023). Standardising Cyber Laws: Global Perspectives and Bangladesh. Dhaka Tribune.

47. Haque, R. (2023). Cyber cell limitations and the need for reform. Dhaka: National Cyber Policy Review.
48. Hossain, M. (2022). Electronic evidence and legal challenges in Bangladesh. Dhaka Law Journal.
49. Islam, K. (2024). Cross-border cybercrime investigations: Challenges in Bangladesh. Dhaka: Law & Justice Review.
50. Kabir, A. (2023). Admissibility of digital evidence in Bangladeshi courts. Dhaka Bar Association.
51. Khan, R. (2024). Budgetary constraints in cybersecurity enforcement. Daily Star Bangladesh.
52. Rahim, N. (2023). Closing loopholes in cyber law: A policy framework. Dhaka: Policy Watch.
53. Rahman, F., & Akhtar, Z. (2021). Internet governance and cybersecurity in Bangladesh. Dhaka University Journal.
54. Sultana, A., & Rahman, A. (2022). Building capacity for cybersecurity: Challenges in Bangladesh. Dhaka: Springer.
55. Ahmed, S. (2021). Cybercrime and legislative gaps in Bangladesh: An overview. Dhaka University Press.
56. Rahman, M., & Karim, T. (2019). Legal responses to cybercrime: Challenges in Bangladesh. Journal of Information and Technology Law, 12(3), 45–56.