UGC & Govt. Approved
Sonargaon University (SU)
সোনারগাঁও ইউনিভার্সিটি (এসইউ)

Research Monograph

On

"Exploring Cyber Crime in Bangladesh: Realities and Challenges"

This Research Submitted for the Partial Fulfillment of the award of the degree in LL.B (Hon's) Department of Law, Sonargaon University (SU), Dhaka.

Prepared For:
Department of Law
Sonargaon University (SU), Dhaka

Supervised By:
Sharmin Jahan Runa
Assistant Professor
Department of Law
Sonargaon University (SU), Dhaka

Submitted By:
A.Q.M Samsuzzaman
ID: LL.B 1902017013
Program: LL.B (Hon's)
Batch: 17th
Department of Law,
Sonargaon University (SU), Dhaka.

Date of Submission: 06/07/2023

Dedication

This Research is dedicated to my
Father & Mother

LETTER OF TRANSMITTAL

To
Sharmin Jahan Runa
Assistant Professor
Department of Law
Sonargaon University (SU), Dhaka.

Subject: Submission of research paper on **"Exploring Cyber Crime in Bangladesh: Realities and Challenges"**

Dear Madam,

It is a great pleasure for me to submit the thesis on **"Exploring Cyber Crime in Bangladesh: Realities and Challenges"** While I doing this thesis, I have tried my level best to make this project paper to the latest standard. I think that thesis paper will fulfill your requirement and pleased you. I, therefore, hope that you would be kind enough to go through this thesis paper for evaluation.

I am always be ready for clearance of any part of my thesis.

Thanking you

A.Q.M Samsuzzaman
ID: LL.B 1902017013
Program: LL.B (Hon"s)
Batch: 17th
Department of Law
Sonargaon University (SU), Dhaka.

CERTIFICATION

This is to certify that the thesis on "**Exploring Cyber Crime in Bangladesh: Realities and Challenges**" is done by A.Q.M Samsuzzaman in partial fulfillment of the requirements for the degree of LL.B. (Honours) from Sonargaon University, Dhaka. The thesis has been carried out under my guidance and is a record of the bonafide work carried out successfully.

……

Sharmin Jahan Runa
Assistant Professor
Department of Law
Sonargaon University (SU), Dhaka

DECLARATION

I do hereby that this Research Monograph on the **Exploring Cyber Crime in Bangladesh: Realities and Challenges** have been done by me and this Research is free from all plagiarism and without help of other. I further declare that this monograph is prepared with my own effort and it was not and never submit to any institute for any academic reason.

A.Q.M Samsuzzaman
ID: LL.B 1902017013
Program: LL.B (Hon‟s)
Batch: 17th
Department of Law
Sonargaon University (SU), Dhaka.

ACKNOWLEDGEMENT

At first, I would like to thank Almighty Allah for his kindness on me in accomplishing the report. I would like to express my deep sense of gratitude to my honorable and distinguished supervisor Sharmin Jahan Runa, Assistant Professor, Department of Law, Sonargaon University (SU), Dhaka for her individual suggestions, valuable time, important information and guidance during the study period that has greatly inspired me in preparing this report successfully.

It could not possible to think all those people who have contributed for the preparation of this report of course there are some very special names that cannot be forgotten. I am also grateful to the Department of Law, Sonargaon University (SU), Dhaka for providing me such an opportunity to come closer to real situation. Finally, I want to express my deep gratitude to my family members and all well wishers whose enormous helps assisted me to complete this report.

A.Q.M Samsuzzaman
ID: LL.B 1902017013
Program: LL.B (Hon‟s)
Batch: 17th
Department of Law
Sonargaon University (SU), Dhaka.

Abstract

People are now able to live in a world without borders and without boundaries known as the cyber world because to the development of internet technology and the widespread use of ICT tools in everyday activities. Computers are being used illegally nowadays for things like espionage via email, credit card fraud, spam, software piracy, and other things that breach our privacy and are offensive to the senses. The main goals of this thesis are to understand the fundamentals of cybercrime and the causes of it, to analyze the various sections of the ICT Act, 2006 that deal with computer and computer-related crimes, to determine whether the police's authority to make arrests without a warrant is reasonable under this Act, and other related goals.The ICT Act of 2006 does not clearly define or describe cyber offenses, police can unlawfully detain people without a warrant, there are only eight cyber tribunals established, so they are unable to adequately serve the needs of the victims, the police are not properly trained, and there is no digital forensic laboratory, among other issues that have been brought to light by this thesis.The ICT Act's provisions relating to section 57 should be changed, and the government should create a separate ministry for this purpose. Additionally, a well-trained cyber police force is necessary to catch cybercriminals, as are sufficient cyber tribunals and one cyber appellate tribunal. The police power of arrest should also be eliminated by amending the ICT Act, and minor and major offences should be identified.

Key Words: Cybercrime, ICT Act, Laws, Bangladesh.

Table of Content

Chapter 1: General Introduction

Serial No.	Topic	Page No.
1.1	Statement of the Problem	8-9
1.2	Research Question	9
1.3	Objective of the Thesis	9
1.4	Literature Review	9-13
1.5	Analytical Framework	13
1.5.1	Role of Legislative Body	13
1.5.2	Role of Lawyers	13-14
1.5.3	Role of Judiciary	14
1.6	Limitation of the Thesis	14-15
1.7	Structure of the Thesis	15

Chapter 2: An Overview of Cybercrime

Serial No.	Topic	Page No.
2.1	Introduction	16
2.2	Definitions of Cybercrimes	16-17
2.3	Origin & Development of Cybercrimes	17-18
2.4	Nature of Cybercrimes	18
2.5	Classification of Cybercrime	18-20
2.6	Reasons behind the Cybercrimes	20-22
2.7	Impacts of Cybercrimes	22
2.7.1	Against Individuals	22
2.7.2	Against Economy	22
2.7.3	Against Society	23
2.7.4	Against Government	23
2.8	Conclusion	23-24

Chapter 3: Laws & Regulations on Cybercrimes in Bangladesh

Serial No.	Topic	Page No.
3.1	Introduction	25
3.2	Necessity of cyber law	25-26
3.3	The Existing Laws of Bangladesh	26
3.3.1	ICT Act 2006(Amendment) Act 2013	27-33
3.3.2	Digital Security Act (DSA) 2018	33-35
3.3.3	Pornography Control Act (PCA) 2012	35-36
3.3.4	The Bangladesh Telecommunication Act 2001	36
3.3.5	The Penal Code 1860	36-37
3.4	Conclusion	37

Chapter 4: Limitations of the existing Regulations & Necessary Recommendations

Serial No.	Topic	Page No.
4.1	Introduction	38
4.2	Limitations of Existing Laws	39-40
4.3	Recommendations	41-42
4.4	Conclusion	42-43

Chapter 5: Conclusion

Topic	Page No.
Conclusion	44-48

Topic	Page No.
Bibliography	49-52

Chapter 1: General Introduction

Statement of the Problem

Cybercrime is such a diverse type of crime that it is best seen as a collection of acts or behaviors. It be unlawful act where in the computer is either as a tool or target or both.[1] This crime is also known as electronic crimes, computer-related crimes, e-crime, high technology crime, information age crime, and so on.

The Internet's creators were unaware that it may one day be used for criminal conduct when they first created the network. Cybercrime is taking place globally in a broad and pervasive way. In order to assess the specialization of cybercrime, the factors that set it apart from regular crime must be taken into account.

"Cybercrime through social media" refers to actions that are also considered offences under Bangladeshi general law. Ordinary law considers harassment to be a crime when it occurs in public and offline, but refers to it as a "cybercrime that happened online" when it is committed online.

Cybercrime is a global crime where crimes are committed across all borders and do not stop at the conventional state-borders. Traditional crimes are initially territorial and committed in the physical world, whereas cybercrime is infinitely territorial and commits them in the electronic or virtual world. The question now is how to deal with these infractions, whether through standard or alternative ways.They can be perpetrated from anywhere and against any computer user in the world."[2]

---

[1]Nagpal, Rohas, *Evolution of Cyber Crimes* (November 22, 2017) Academia.edu https://www.academia.edu/35222024/Evolution_of_Cyber_Crimes_Rohas_Nagpal_Asian_School_of_Cyber_Laws.

[2] Goodman, Marc D and Susan W Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace* Full text of "The Emerging Consensus on Criminal Conduct in Cyberspace" https://archive.org/stream/TheEmergingConsensusOnCriminalConductInCyberspace/TheEmergingConsensusOnCriminalConductInCyberspace_djvu.txt.

The rules governing crimes using computers, computer networks, the Internet, electronic devices, e-commerce or e-business, cyber security, and other similar technologies are covered by cyber law. Cyber laws safeguard communications, intellectual property rights, Internet trade, taxes, consumer protection, advertising, censorship, and free expression. Because it deals with the relationship between the Internet and technological and electrical elements including computers, software, hardware, and information systems.

Research Question

How effective is the law in dealing with cybercrimes in Bangladesh?

Objective of the Thesis

The main goal of this dissertation is to identify the influence of cybercrime in Bangladesh in terms of technological advancement. The primary goal of the study is to determine the true scenario and examine the cybercrime committed in various sectors. It also aims to revisit the legal measures and strategies implemented in Bangladesh to combat cybercrime, and to make possible suggestions for cybercrime protection.

Literature Review

FawziaCassim in her article "Formulating specialized legislation to address the growing specter of cybercrime: A comparative study" author looks at the cyber legislation formulated to address cybercrime in the United States of America, The United Kingdom, Australia, India, The gulf Countries and South Africa.[3] The study reveals that the inability of national laws to address the challenges posed by cybercrime has led to the introduction of specialized cyber legislation.[4] It is advocated that countries should introduce new cyber laws to respond to the rapid change in technology and cybercrimes.[5] There should be continuous research and training of IT security

[3]Cassim, Fawzia, *Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study*https://www.researchgate.net/publication/317904403_Formulating_specialised_Legislation_to_address_the_Growing_Spectre_of_Cybercrime_A_Comparative_Study.

[4]*Ibid.*
[5]*Ibid.*

personnel, financial service sector personnel, police officers, prosecutors and the judiciary to keep them abreast of the evolving technology.[6]

The author claims in her work that the lack of publicly available information on the majority of cybercrime types is a significant challenge for cybercrime experts. Cybercrime investigations are hampered by the absence of unified international standards for evidence requirements, mutual legal assistance in cybercrime cases, and timely collection, preservation, and sharing of digital evidence between nations. Many digital devices have proprietary operating systems and software making it necessary to use specialized tools to find, collect, and store digital evidence.

I agree with the author that there is no harmony between the laws and the authority based on this observation. The main question, in my opinion, is whether and how far this rule extends to cybercrime. The United Nations should establish a global agreement or Protocol that includes solutions aimed at addressing global challenges in order to achieve global harmonization of cybercrime legislation and a common understanding of cyber security and cybercrime among countries at all stages of economic development.

An Addl. Dist. & Sessions JudgeTalwant Singh in his writing "Cyber Law & Information Technology" has taken up a crucial and rare topic of discussion that is the importance of harmony between the law enforcement agencies and computer professionals.[7] According to author both the parts are equally important for enabling strong cyber security in country and make internet a safe place for its users.[8]

The author claims that one barrier to conducting cybercrime investigations is the law enforcement agencies' present, constrained capacity to do so. Such an approach is ineffective due to the widespread use of information and communication technology in criminal investigations. A lack of knowledge of the rights and laws made for the country's citizens can even cause the slowing and affecting of India's chain of justice delivering system.

---

[6] *Ibid.*

[7] Singh, Talwant, *CYBER LAW & INFORMATION TECHNOLOGY*https://www.coursehero.com/file/22091388/cyberlaw/.

[8] *Ibid.*

I agree with the author. From my observation, Bangladesh has taken a constructive approach by developing rules and laws to protect cyber victims, but cybercrime appears to be a low priority for the police. A highly competent and exceptionally well-equipped law enforcement organization is essential to combating cybercriminals. For the good of the public, it is important to restrict and outlaw a variety of offensive websites.

S.R. Khan in his article "Cyber law in Bangladesh through an international lens" claims that one of the biggest criticisms directed at the existing cyber law framework in Bangladesh is that the particularly controversial provisions of the Digital Security Act, 2018 (DSA), and the preceding Information and Communication Technology Act, 2006 (ICT) were inconsistent with Bangladesh's international law obligations.[9] Many journalists, human rights defenders and academics think that the DSA is unduly restrictive of the right to freedom of expression on the internet.[10]

The aim of the digital security legislation was to address cybercrime and punitive processes. However, a review of the Digital Security Act of 2018 paints a different picture in the two and a half years since its start.[11] According to data research, 197 cases were brought under this legislation last year, with the majority of them including claims such as "rude language," "defamatory utterances," "sharing distorted photographs," and "conspiracy against the government".[12]

The author claimed that the legislation empowers the government to order the removal and blockage of any material or data on the internet that it considers essential, giving it vast authority to silence people who criticize its policies or share information about human rights breaches in the nation. Fourteen of the law's twenty clauses dealing with charges and penalties make defendants ineligible for bail, allowing the accused to be held forever.From this point of view I totally agree with the author.

---

[9] Khan, SifatRahbar, *Cyber Law in Bangladesh through an International Lens* (April 29, 2022) The Business Standard https://www.tbsnews.net/thoughts/cyber-law-bangladesh-through-international-lens-411742.

[10] *Ibid.*
[11] *Ibid.*
[12] *Ibid.*

However, in other side, the author did not mentioned about anything about the rectification or modification of the existing laws and regulations or implementation of any new law. From this point, I have disagreement with the author because rectification of existing laws become a necessary to avoid many disputes and crimes.

Md. Abu Hanif in his journal "Cybercrime and Cyber Law: Growth of The State Concerns and Initiatives in Bangladesh" mentioned some reasons for the vulnerability of computers and high tech crimes such as- Capacity to store data in comparatively small space; easy to access to codes, advanced voice recorders, retina imagers etc.; complexity in understanding the computer operating systems; negligence in protecting the computer system; and loss of evidence.[13]

The author is highlighting the common problems of cyber related issues. Though these reasons are obviously accurate but there are more reasons which make a gap between the thought of the author and mine. From my point of view, drawbacks in judiciary system is one of the major reason behind cybercrimes which cause disagreement between the author and me and for that reason, my thesis is different from the author.

This dissertation sheds light on the obstacles that prevent effective investigations into cybercrime, including the lack of unified international standards for evidence requirements (both in terms of admissibility in court and in terms of international state responsibility), mutual legal assistance in cybercrime cases, and the timely collection, preservation, and sharing of digital evidence between nations. Cybercrime investigators often encounter technical challenges. Another obstacle to conducting cybercrime investigations is the law enforcement agencies' limited ability to carry out these investigations. These limited law enforcement capacities are made worse by the short lifespan of cybercrime investigators' expertise. Additionally, in what is described as a "skills deficit," highly skilled and competent cybercrime investigators are leaving government and national security institutions to work in the private sector, which pays better for their knowledge, skills and talents.

---

[13]Hanif, Md. Abu, *Cybercrime and Cyber Law: Growth of the State Concerns and Initiatives in Bangladesh* (2018) http://www.aasmr.org/liss/Vol.5/Vol.5_No.2_2.pdf.

Analytical Framework

Role of Legislative Body

Bangladesh's parliament passed the Telecommunication Regulation Act in 2001 to combat cybercrime using telecommunications means. Later, the Information and Communication Technology (ICT) Act of 2006 was enacted, which specifically outlined the investigation and trial mechanism for online offenses. In 2014, the ICT Division issued the Information Security Guidelines and the National Cyber Security Strategy to protect national cyberspace.Unfortunately, no substantial national progress has been discovered with the ICT Act and NCSS, despite the fact that internet usage is rapidly expanding. Bangladesh's cybercrime laws are woefully inadequate and ill-equipped to deal with the growing threat posed by cybercrime via computer, internet, or social media. Ineffectiveness and flaws in national legislation have thrown the nation's cyber security into disarray. By failing to bring wrongdoers to justice, these disparate laws have broadened the scope of cyber violence in Bangladesh.

The reason for selecting this criteria is that the Legislatives can play a vital role to reduce the cybercrime offences by imposing proper laws and regulations; so that the number of cases relating to cybercrime will be decreased eventually. In this paper, we can analyze the role of Legislative Body of the government whether they need to amend the existing law and will also try to discuss the role and effectiveness of the different governmental agencies in case of protection of the victims.

Role of Lawyers

Cyber law is a difficult and evolving field of the law. Cyber attorneys frequently work on matters that are critical to their clients. Developing privacy and security rules for a large corporation has ramifications for the entire organization. High stakes are frequently involved in domain disputes, job problems, and contract disputes. Lawyers who desire to influence laws and policies may appreciate having a voice. Litigators and transactional attorneys with a wide range of practice skills and interests are also welcome.

In this dissertation, this criteria will be utilized to determine the variables that a court considers before recognizing and proclaiming a person as an offender and evaluating the type of his cybercrime by hearing the lawyers' arguments. The case laws and judgments will be researched

in order to assess the issue using the criteria of the legal community's function. Analyzing the function of attorneys will help this dissertation in determining the practicality in the implementation of laws, identification of victims and remedies, as well as the penalties of wrongdoers in court.

Role of Judiciary

Bangladesh's judicial system is experiencing a number of issues as a result of the nature of cybercrime. The laws are insufficient, but the policy and operational systems are hampered by a lack of expertise. Judiciary plays a critical role in the protection, safety, and rights of women in cyberspace. Bangladesh's Judiciary has been working to remedy the gaps in the Digital Security Act, 2018.However, in a changing context, numerous types of new advances in cyberspace lead to various types of cybercrimes that go undiscovered. As a result Bangladesh need such cyber-savvy judges who could readily handle and appropriately justify cybercrime.

In this dissertation, this criteria will be utilized to assess if courts implement the laws and principles to accomplish justice via fairness of the outcome. It will aid in determining whether the courts were able to provide victims with fair justice. The relevant case laws will be examined in order to assess the preservation of victims' privacy, the amount of harm sustained, and the restoration of society. The criterion will aid in examining the function of the judiciary in filling the current legal gap as well as analyzing its role when there is a legal vacuum. This criterion will be used to examine the role of judges in promulgating cyber security and victim redress.

Limitation of the Thesis

Considering the nature of the work, an analytical and empirical research approach was used to finish it. For this objective, primary and secondary data sources have been considered. The references were taken from national and international updated legislation, books by well-known authors, publications published in reliable journals, decided cases, research reports, acts, newspapers, and websites, among other sources. Due to the unstable situation of our country and lack of time it was not possible to take interviews of the experts and the victims. Unavailability of proper relevant literature, resources and contributions could be another major limitation. This paper intends to hammer out the reality of cybercrime and the national, regional, and worldwide state of cyber laws, exposing flaws and making suitable recommendations to address the

problems of combating various types of cybercrime. Though the topic is very common but due to the faulty laws of our country it would be a challenge for the author to come up with a proper solution.

Structure of the Thesis

The second chapter will give an overall idea about cybercrime.Understanding the terminology and context of cyber laws, it is essential to understand cybercrime. This chapter will assist you in fully comprehending it. This chapter will also describe the causes and consequences of cybercrime in many areas of society.

The third chapter will concentrate on existing national rules and regulationsof our country. In this chapter I will try to identify the flaws of those laws as well as the inconsistency of them with the international laws.

In the fourth chapter I will discuss the limitation of the existing laws along with their causes. There will also be the suggestion or advice to build a secured cyber-system and cyber laws.

The findings of each chapter will be summarized in Chapter five. It will be the dissertation's conclusion comment. It will also present the study's findings.

Chapter 2: An Overview of Cybercrime

Introduction

We are becoming increasingly dependent on the online system as we digitalize every industry day by day. The question of how secure the internet actually is arises as more and more industries become reliant on it. Data theft, financial sector electronic fraud, identity theft, unauthorized use of sensitive information, hacking or cracking, cyber stalking, the distribution of pirated software, terrorism, credit card fraud, spamming, e-money laundering, ATM fraud, and phishing.

The most effective preventive measure to control this type of contemporary crime is modern legislation, which addresses all aspects of cybercrime and may be construed to account for emerging dangers.If we define cybercrime as acts that are punishable by the information technology act that would not suitable as penal code of some counties cover many cybercrime.[14]

Every crime has a unique impact on the society in which it occurs as well as on the global community and cybercrime is not beyond that. It is undoubtedly a product of computer technology and is strongly tied to the internet.

This chapter will define cybercrime and cyber laws, as well as their origins. This chapter will also help to identify the cyber criminals and will illustrate thenature, characteristics and classifications of cybercrime.

Definitions of Cybercrimes

[14]Karzon, Hafizul Rahman, *Theoretical and Applied Criminology* (Palal Prokashoni1st ed2004) 411.

Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.[15]

Cybercrime is a broadly used term to describe criminal activity committed on computers or the Internet. Some of it is punishable by the laws of various countries, whereas others have a debatable legal status.[16]

The Oxford English Dictionary defines:

"Cybercrime as a crime committed using computer or internet. Although the term cyber is technically limited to crimes involving the internet, it is used more broadly to refer crimes committed using stand-alone computers."[17]

Cybercrime is a transnational crime that has an international reach. Institutions, law enforcement organizations, and other stakeholders are gravely concerned about the complexity of cybercrime assaults and the security of information available online.

No statute or Act passed or enacted by the Bangladeshi Parliament contains a definition of this term. The increasing reliance on computers in modern life is the root of the evil known as cybercrime. Cybercrime has taken on fairly frightening overtones in the modern day, when everything from microwaves and refrigerators to nuclear power plants is run by computers.

Origin & Development of Cybercrimes

The origin of cybercrime may be traced back to the mainframe computer era, which is also when computers were invented. Professor Susan W. Brenner separated the history of cybercrime into two periods in his book on the subject. The first period covered the years from the mainframe computer era until 1990, when the internet and personal computers were becoming more advanced and commonplace.[18] The second period spans from 1990 until the present.[19]More

---

[15]*Cybercrime*Cybercrime Definition <https://techterms.com/definition/cybercrime>.

[16]Chaubey, RK, *An Introduction to Cyber Crime and Cyber Laws* (Kamal Law House1st ed2009) 135.

[17]Grabosky, Peter N, *Electronic Crime* (Pearson Prentice Hall1st ed2006) 2.

[18]Brenner, Susan W, *Cybercrime Criminal Threats from Cyberspace (2010* (Praeger1st ed2010) 46.

easily we can divide the origin of Cybercrime in two periods, one, before the internet and the other after emergence of Internet, because 1990 was the time when internet was spreading very fast around the globe.[20]

Nature of Cybercrimes

The threat of cybercrime is constant and ever-evolving. Cybercrime differs most from traditional crime in that it is anonymous and without geographical boundaries. Identity theft, the dissemination of photographs of child sexual abuse, internet auction fraud are all examples of cybercrimes. Due to scattered pieces in several locations, it is very difficult to gain a complete picture of the entire criminal process.

A cybercriminal can take down websites and portals, commit online frauds by sending money around the world, access highly sensitive and confidential data, harass people via obscene or threatening emails, play tax scams, engage in child-targeted cyber-pornography, and commit countless other crimes. Nobody is supposed to be secure in the digital world. Cybercrime would have an impact on all of us as Internet usage grows, either directly or indirectly.

Classification of Cybercrime

Cybercrimes are crimes done on, via, or with the use of the internet. These include lying, cheating, fraud, misrepresentation, defamation, pornography theft, etc. Internet-related crimes like hacking and virus distribution are a recent development. Old crimes are utilized to commit new ones. For instance, when hacking is done to perpetrate online scams.

i) Hacking

„Hacking" means unauthorized access to a computer system. It is the most common type of Cybercrime being committed across the world. The word „hacking" has been defined in *section 56 of the Information & Communication Technology Act 2006,* as follows:

"Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any Act and thereby destroys, deletes or alters any

[19] *Ibid* 20.

[20] *Ibid*23.

information residing in a computer resource or diminishes its value or utility or affects in injuriously by any means commits hacking."[21]

ii) Cyber Pornography

The internet has made it possible to spread crimes like pornography. On modern media, such as hard drives, floppy discs, and CD-ROMs, pornographic content may be copied more swiftly and inexpensively. There are more serious offences that are universally condemned, such child pornography, and are far simpler for criminals to conceal and spread through the Internet.

iii) Cyber Stalking

Cyber stalking is the practice of a cybercriminal repeatedly harassing or threatening a victim while utilizing online services. In general, stalking refers to a pattern of harassment directed at the victim, such as following them, making threatening phone calls, damaging their property, or leaving notes or objects behind. The crime of stalking must be taken seriously since it may be followed by significant violent activities like harming the victim physically.

iv) Cyber Terrorism

The employment of disruptive actions, or the threat of doing so, in cyberspace with the goal to achieve social, intellectual, religious, or political objectives, or to terrorize anybody in promotion of such objectives, is known as cyberterrorism. Computers play the role of a contemporary robber who can steal more with a computer than with a rifle. Terrorism undoubtedly combines the greatest phobias; the dread of arbitrary, violent victimization blends nicely with the mistrust and outright dread of computer technology.

v) Cybercrime related to Finance

Cybercriminals, often known as fraudsters, employ a variety of strategies and schemes to deceive other users of the internet in order to commit one of the many forms of cybercrimes that are directly tied to obtaining money or money by illicit means. One of the most profitable industries expanding in the internet nowadays is online fraud and cheating. It might take on several shapes.

[21] Ahmed, Dr. Zulfiquar, *A Text Book on Cyber Law in Bangladesh* (National 6aw Book Company1st ed2009)63-64.

Internet auction frauds, contract crimes, investment scams, job postings, and other types of online fraud and deceit are only a few of the incidents that have come to light.

vi) Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets, academic certificates etc. are made by criminals using sophisticated computers, printers and scanners. Whoever makes any false documents or electronic record part of a document or electronic record with, intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

vii) Cyber Defamation

Cyber defamation means making or publishing any defaming information or imputation concerning any person, by electronic form with internet to harm or knowing or having reason to believe that it will harm the reputation of such person or defame him.The basic difference between defamation and cyber defamation lies in the modes through which defamation is committed. Section 499 of Penal Code only contains the traditional forms of committing defamation. But in the era of technology, defamation can be committed through the use of ICT tools such as internet, email.

ix) **Intellectual property crimes / Distribution of pirated software**

A collection of rights comprise intellectual property. An offence is any unlawful conduct that wholly or partially denies the owner their property rights. Software piracy, copyright infringement, trademark and service mark infringement, theft of computer source code, etc. are examples of prevalent IPR violations.A wide range of wrongdoings fall under the general category of "digital wrongdoing," and it's possible that the extent and severity of the infractions may eventually call for a variety of laws to address them.

Reasons behind the Cybercrimes

The computer has excellent standards for storing information in a small space. This means that it is less demanding to evacuate or infer data across physical or virtual media. Key loggers that can steal access codes, voice recorders, retina imagers, and other devices that can fool biometric frameworks can get past firewalls. Legal guidelines are necessary to safeguard computers from cybercrime.The reasons for the vulnerability of computers may be said to be:

1) **Complex**

The Computers deal with functioning frameworks, which are constructed from a sizable quantity of programs. It is preposterous that there won't be a slip-by at any arrangement since human nature is brittle. These holes are exploited by the online thieves, who get access to the PC architecture.

2) **Capacity to store data in comparatively small space**

The computer has the special ability to store data in a very little amount of space. It is made considerably simpler by the capacity to delete or derive information using either a physical or virtual media.

3) **Confidential Information**

Online and on networks, private information is kept from security companies, academic databases, financial institutions, and even governmental entities. Because of this, cybercriminals are able to start an illegal access and exploit it to suit their purposes. Security codes, bank accounts, and other information can be accessed by thieves through the manipulation of sophisticated technology and the bypassing of firewalls.

4) **Complexity of Codes**

Operating systems contain sophisticated codes that may be cracked or tampered with to get into the system. Security is never completely foolproof, and a skilled hacker can always find a way around it. A cyber thief is similar to a typical bank robber in that he studies the security system and exploits it, with the exception that he can break security virtually.

5) **Negligence**

Sometimes, basic carelessness may lead to illegal activity. Examples include keeping a password on a work computer, utilizing work data in public, and simply storing data without encryption. Such carelessness might be used by the cybercriminal for the purpose of gathering, manipulating, and fabricating information.

6) Lack of Evidence

The absence of evidence to prosecute criminals in court is one factor contributing to an increase in cybercrime. There are so many techniques to cover up the evidence of a cybercrime, yet so little is done to actually catch the offender. Think of a pedophile who uses social media or email to lure their victim. The police can follow the information to the offender, but the trail cannot be utilized in court until strong physical proof is discovered.

7) Easy to Access

There is always a chance that a breach might occur, not because of human mistake but because of the sophisticated technology, which makes it difficult to protect a computer system from unwanted access. Key loggers that can steal user credentials, sophisticated voice recorders, retina imagers, etc. that can trick biometric systems, and even firewall-bypassing logic bombs can be used to get past numerous security measures.

Impacts of Cybercrimes

Against Individuals

Cybercrimes committed against people include various crimes like transmission of child-pornography and harassment through e-mail.[22] The trafficking, distribution, posting, and dissemination of obscene material including pornography constitute one of the most important cybercrimes known today.[23] Cyber harassment is a distinct cybercrime.[24] Harassment can be sexual, racial, religious, or other.[25] This also brings us to another related area--violation of citizen which is a crime of grave nature.[26]

---

[22]Mia, Badsha, *Cybercrime and Its Impact in Bangladesh: A Quest for Necessary Legislation* (July 1, 2015) Academia.edu https://www.academia.edu/13465468/CYBERCRIME_AND_ITS_IMPACT_IN_BANGLADESH_A_QUEST_FOR_NECESSARY_LEGISLATION.

[23]*Ibid.*
[24]*Ibid.*
[25]*Ibid.*
[26]*Ibid.*

Against Economy

The most damaging cybercrimes are those that target the economy. E-commerce and other internet-based commercial activity have made this possible. The following list of cybercrimes targeting the economy includes- cracking, phreakers, malicious programs etc.

Against Society

Socially, cybercrime primarily affects emerging and underdeveloped nations. As previously stated, handling, prosecuting, and investigating cybercrime is an expensive process. Because developing and underdeveloped countries are the target of the majority of these crimes, they must allocate funds for this area while neglecting other crucial social projects for the good of society. Therefore, governments and individuals suffer in two ways: first, by being targets of cybercrime, and second, by having public resources allocated to its prevention while disregarding other national issues or programs.Some cybercrimes against society are porno mailing, pornography, defamation, spreading racial and other hate propaganda through internet etc.Since of the fear and insecurity that the public feels, there is another societal consequence of cybercrime because, in certain cases, people refrain from using technology to protect themselves from criminal activity. In this age of globalization, this might have an impact on how individuals socialize, which closes the doors to fortune for many.

Against Government

One specific type of crime in this category is cyber terrorism. The expansion of the internet has demonstrated that both people and organisations are using cyberspace as a means of threatening and terrorising national and international governments. When someone "cracks" into a website that is managed by the government or the military, this crime emerges as terrorism. The political climate of every nation is undoubtedly negatively impacted by the increased frequency with which websites belonging to governmental bodies and political parties are hacked worldwide.

Conclusion

The number of cybercrimes is rising daily and come in many different forms. Hackers, cybercriminals, online criminals, and other people with similar names utilize the internet and computers in a harmful, disruptive manner. Due to a lack of knowledge or infrastructure, many

cyber-attack incidents go undetected. It poses the threat of starting a financial crisis, a national uprising, the suspension of services, etc.

Cyber criminals take full advantage of the Internet's anonymity, secrecy, and interconnection, assaulting the fundamental underpinnings of our contemporary information society. They carry out cyber-attacks using numerous attack vectors and are continuously looking for new tactics and strategies to achieve their aims while evading notice and imprisonment. Because of the dynamic nature of cyberspace, creating and enforcing cyber laws present several difficulties.Most cybercrimes are committed with the intention of financial benefit by the attackers, however the methods by which cybercriminals hope to be paid differ. Financial losses might be enormous as a result of cybercrime, but organizations can also suffer other negative repercussions. Businesses may limit their vulnerability by implementing an effective cyber security strategy that employs a defense-in-depth approach to safeguarding systems, networks, and data.

The existing national rules and regulations and their flaws relating to cybercrimes will be discussed in the next chapter.

Chapter 3: Laws & Regulations on Cybercrimes in Bangladesh

Introduction

Hart in his work "The Concept of Law" has said, "human beings are vulnerable so rule of law is required to protect them."[27] Applying this to cyberspace, we may conclude that computers are susceptible, and that the rule of law is needed to secure and safeguard them from cybercrime.

Cybercrime poses a number of difficulties to traditional criminal law and the criminal justice system as a whole. The first difficulty is in defining it. In reality, the trendy title of cybercrime encompasses a wide range of offences. This conceptual framework has had a substantial impact on worldwide and national cybercrime legislation, particularly Bangladeshi policies.

Many governments have taken use of the potential provided by ICT within a policy framework in recent years, establishing guidelines and preceding the construction of a national ICT strategy as part of the broader national development plan. Bangladesh plans to leverage ICT as a fundamental driver of socioeconomic growth.

In this chapter I will discussed about some cyber offences in our country. This chapter will also cover the existing national laws and regulations along with their limitations regarding cybercrimes. Moreover, at the end, some specialized agencies and their activities regarding cybercrime issues will also be discussed.

Necessity of cyber law

In today's technologically advanced world, the globe, and crimes, are getting increasingly digitally sophisticated. The Internet was first designed as an uncontrolled research and information exchange platform. As time went, it got more transactional, with e-business, e-commerce, e-governance, and e-procurement, among other things. Cyber laws address all legal concerns of internet crime. As the number of internet users increases, so does the demand for cyber laws and their implementation.

---

[27] Hart, HLA, *The Concept of Law* (Oxford University Press Inc.2nd ed1994).

When the Internet concept was invented and further evolved, little did the developers realize that the Internet would have the capacity to turn into a monster capable of being used for a variety of unlawful and immoral actions, and that it would eventually need to be regulated. Identity theft, terrorism, and money laundering are just a few of the unpleasant things that happen in cyberspace. Because of the Internet's anonymity, anybody may engage in a wide range of illicit behaviors with impunity. Individuals, businesses, and others are using these "grey zones" to do unlawful acts in online, necessitating the need for cyber laws. As a result, Cyber Law affects us in our daily lives.Every action we do in cyberspace may and will be viewed from a legal viewpoint since the Internet is evolving and is now thought to be the best medium to have ever evolved in human history.

Every moment of every day, there are different Cyber Law problems at play whether we register our email, book an online train ticket, engage in some electronic commerce, open a bank account, take money out of an ATM, or pay our utility bills. These problems might not disturb us, and we might believe that these regulations are far away from us and have no impact on online activity.However, sooner or later, a procedure may not respond, resulting in a loss, and we will be compelled to pay attention to cyber law for our own advantage.

The Existing Laws of Bangladesh

Despite the fact that Bangladesh is a third-world country, the number of Internet users is rising due to the availability of smart phones. As a result, cybercrime is steadily expanding throughout the country. To combat cybercrime, the government is also enacting laws and raising public awareness, among other things.

The cybercrime related laws of Bangladesh are briefly discussed below:

Information and Communication Technology (ICT) Act 2006 (Amendment) 2013

On October 8, 2006, the Bangladesh Nationalist Party (BNP) and Jamaat-i-Islami (JI) government enacted the ICT Act for the first time.[28]This **ICT Act, 2006** contained a variety of unclear, imprecise, and overbroad clauses that serve to criminalize the use of computers for a

[28]*ICT Brief Final Draft 20 November 2013*Scribdhttps://www.scribd.com/document/269184617/ICT-Brief-Final-Draft-20-November-2013.

wide range of activities that violate international law's protection of the right to free speech, including the right to receive and impart information. Although the right to information is not absolute, the constraints envisioned by the Act do not come within the spectrum of exceptions authorized under international law, including Bangladesh's treaty commitments. Section 46 of the original ICT Act, for example, gives the government the authority to instruct any law-enforcing agency to restrict information accessed via any computer resource if in their opinion such prevention is:

"…*necessary or expedient so to do in the interest of the sovereignty, integrity, or security of Bangladesh, friendly relations of Bangladesh with other States, publicorder or for preventing incitement to commission of any cognizable offence."*[29]

Section 57 of theICT Act 2006made publishing or sending, or inducing others to publish or transmit, a crime. *"...any material which is fake and obscene or its effectis such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, toread, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence."*[30]

The original ICT Act's provisions, notably Section 57, are incompatible with Bangladesh's duties under Article 19 of the ICCPR. The stipulated offences are imprecise and overbroad; the limits on freedom of thought and expression go beyond what is authorized under Article 19(3) of the ICCPR; and the restrictions are not necessary or proportionate to accomplish a legitimate goal.

Before registering a case under the statute, the police had to obtain authorization from the Home Ministry under the original Act. Sections 54, 56, 57, and 61 of the revised Act have been rendered cognizable, allowing police to conduct arrests without a judicial warrant.

[29] *Bangladesh National Parliament - SAMSN*https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf.

[30] *Ibid*

Then, on October 6, 2013, after the cabinet had approved the draft on August 19 of same year, the Awami League (AL)-led government enacted **the ICT (Amendment) Act 2013**.[31]

The Act and its Amendment have drawn criticism for a variety of reasons, including potential harm to democracy, restrictions on human rights, and restrictions on freedom of speech, particularly freedom of the press. This new Act renders the law even less human rights compliance with Bangladesh's duties.

Under the modified Act, offences mandated by sections 54, 56, 57, and 61 have been declared non-bailable, which implies that bail cannot be granted automatically but must be granted at the discretion of the court. Finally, the modified Act raised the maximum term for offences under sections 54, 56, and 57 of the Act up to 14 years, with a seven-year minimum sentence. The new law also keeps the optional penalties of one crore taka in place.

At the national level, Bangladesh's Constitution protects freedom of expression with some acceptable constraints under Article 39. Article 39 of the People's Republic of Bangladesh Constitution guarantees the right of every citizen to free speech and expression, subject to any reasonable limits imposed by law in the interests of the State's security, friendly relations with foreign governments, public order, decency, or morality, or in connection to contempt of court, defamation, or incitement to an offence.[32]Recognizing it as a constitutional right, the second paragraph of the Article states that the right is protected subject to any justifiable legal constraints.

The Universal Declaration of Human Rights (UDHR) of 1948 and the International Covenant on Civil and Political Rights (ICCPR) of 1966 both provide freedom of expression or speech.Article 19 of the UDHR says: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[33] In the same vein, article

---

[31]Alam, Shahid, *Fathoming ICT (Amendment) Act, 2013* (March 7, 2015) The Daily Star https://www.thedailystar.net/fathoming-ict-amendment-act-2013-14762.

[32]*The Constitution of The Peoples' Republic of Bangladesh* art 39

[33]*Universal Declaration of Human Rights* United Nations https://www.un.org/en/about-us/universal-declaration-of-human-rights.

19 of the ICCPR says: "Everyone shall have the right to hold opinions without interference. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." [34]And, this right may "be subject to certain restrictions, but these shall only be such as are provided by law and are necessary."[35]

The International Court of Justice is worried that the revisions may stifle lawful public expression by journalists, human rights advocates, and others, including expression critical of the government.[36] The ICJ requests that the Bangladeshi Parliament repeal the Information and Communication Technology Act (2006), as modified in 2013, or alter the ICTAct to put it in accordance with international law and norms, particularly Bangladesh's legal duties under the ICCPR. At the very least, this would necessitate.[37]

Sections 54, 56, 67, and 61 became cognizable and non-bailable as a result of the 2013 change, whereas Sections 55, 58, 59, 60, 62, 63, 64, and 65 became non-cognizable and bailable. Because of this, there have been substantial changes in how cases are brought and who decides what is included by the Act's punitive provisions. It gives the police unrestricted power to more regularly intervene in the private-personal lives of residents, taking us one step closer to a controlled society. Whereas other democratic nations are attempting to restrict police intervention in private life, this additional police powers would undoubtedly stymie that effort. This raises the question whether the police have the necessary skills to deem an internet comment or logical explanation written in a post to be offensive and disparaging.

Furthermore, article 57 has been a source of great worry for them, part of which reads: "…any willful release on websites or any other electronic platform of any material which is false, vulgar,

---

[34]*International Covenant on Civil and Political Rights* OHCHR https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[35]*Ibid.*

[36]Khattab, Asser, *Bangladesh: Information and Communication Technology Act Draconian Assault on Free Expression* (November 20, 2013) International Commission of Jurists https://www.icj.org/bangladesh-information-and-communication-technology-act-draconian-assault-on-free-expression/.

[37]*Ibid.*

defamatory and liable to cause deterioration of law and order, or tarnishes the image of the state or individual, or hurts religious sentiments is treated as a cybercrime."[38]

According to Section 57 of the Act, the majority of the cases up to this point were filed. In addition to the Pornography Act, there have also been a few instances of computer system hacking and the online publication of pornographic content. As a blatant violation of the freedom of speech and the right to privacy protected by Articles 39 and 43, this frequent application of Section 57 has alarmed writers, journalists, bloggers, and human rights activists. 57(1) of the Act very loosely defines the offence as: "If any person deliberately publishes or transmits or causes to be published or transmitted in the website or in any other electronic form any material which is false and obscene and if anyone sees, hears or reads it having regard to all relevant circumstances, its effect is such as to influence the reader to become dishonest or corrupt, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity will be regarded as an offence."[39]

If we look at Section 57(1) on its own, we can observe that it does not include particular offences, including the age range that will view, hear, or read the content. A minor's comprehension level could not be the same as an adult's. The police officer is also the most likely person to see, hear, or read now that the new adjustments have been made. As was previously said, the police may not be able to develop a reasonable answer for what he observes, hears, or reads online given his academic credentials.

Additionally, defamation is a crime that is covered under Provisions 505 and 505A of the Penal Code, and those sections only impose a 2 year sentence or a fine or both.[40] However, the ICT Act's Section 3 specifies that its requirements have precedence over all other laws.[41]

---

[38] বাংলাদেশ উটারকাউন্সিল (বিসি)বাংলাদেশ উটারকাউন্সিল (বিসি)-গণপ্রজাতন্ত্রীবাংলাদেশরকার https://bcc.gov.bd/site/page/31309623-287a-4430-811b-d354f6d6cbeb/ICT- Act-2013.

[39] *Ibid* s 57(1).

[40] *The Penal Code 1860*s 505, 505A.

[41] *The ICT (Amendment) Act 2013*s 3.

According to Section 57(2) of the previous Act, violating Subsection 1 of Section 57 will result in a 14-year sentence in prison, a fine of Taka onecrore, or both.[42] The 2013 amendment increased the sentence from 10 to 14 years in jail.[43]I am interested in hearing from anyone who would initiate a prosecution under the Penal Code now that Section 57(2) of the ICT Act provides for 14 years in prison and a fine of taka one crore.

The clause goes on to mention the risk of harming or causing harm to religious beliefs, as well as inciting violence against any person or organization. Surprisingly, the section again failed to specify what constitutes a violation of one's religious beliefs, and why would incitement against any individual or organization be represented in a single section.The right to choose one's religious beliefs is guaranteed under the nation's constitution. This unquestionably includes the option to reject all religions and maintain one's freedom. There have always been issues with this interpretation. The liberal view was not given enough sway because of social and political pressure. As a result, it is always possible to harm someone for having no particular religious beliefs. The non-believers are not given any room under the other State legislation either.

Additionally, Section 205 of the Penal Code lays forth the penalties for publishing any materials that harm someone's religious beliefs.[44] If this is done through the publication of a book or pamphlet, the offender faces a 3-year jail sentence.[45] If the same is posted online, there will be a 14-year prison sentence and a TK $1 billion punishment, as per Section 57 of the ICT Act.[46] The subject of releasing fraudulent or offensive content under false pretenses in order to harm another person is not addressed in the section. Anyone may purchase a false Identity on social media and publish fraudulent and offensive content while posing as another individual.In that instance, there is no way to determine who actually started the account because the credentials used to open the account will point the investigating officer to the person it was opened for.

[42] *The ICT Act 2006* s 57(2).

[43] *The ICT (Amendment) Act 2013*s 57(2).

[44] *The Penal Code 1860*s 205.

[45] *Ibid.*

[46] *The ICT(Amendment) Act 2013*s 57.

Defaming somebody is prohibited, according to Section 57.[47] The Penal Code of Bangladesh, which only imposes a 2-year sentence, also defines this.[48] But the ICT Act of 2013 mandates for either a 14-year sentence or a fine of Tk. 1 billion, or both.[49]In that case, if someone publishes any materials (other than on the internet) that are defamatory of anyone, they will still be held accountable under the Penal Code's provisions. However, if they do so online, such as on their blog or Facebook page, they will be held accountable under Section 57, which carries a punishment that is ten times greater than the Penal Code. Why there is prejudice for the same offence is unknown.

Statistics published by the Cyber Security Tribunal show that, between 2013 and 2017, 740 cases were submitted nationwide under the ICT Act, with 60% of those cases being brought under the contentious Section 57.[50] Up of September 2017, the Dhaka Cyber Tribunal had more than 450 cases pending in relation to them.[51] On September 1, 2015, the High Court (HC) issued an order requesting that the government provide justification for not declaring Section 57 of the ICT Act unlawful within four weeks.[52]Section 57 of the Act of 2013 won't be repealed, according to the government of Bangladesh. The administration argued in favor of this clause by saying it would serve as a "safeguard" for the government. Without Section 57 of the Act of 2013, the government believes that it would be impossible to combat cybercrime and that the number of such instances would increase. The section must be utilized against anyone spreading false information. So, it continues to be a weapon for oppression, and it is expected that the future administration won't change or repeal the Act since it provides the ideal instrument for tyranny.

Digital Security Act (DSA) 2018

Apparently replacing the contentious Section 57 of the 2006 Information and Communication Technology Act, the Digital Security Act (DSA) was passed in 2018 (asamended in 2013). In contrast to the previous legislation, the new one adopts a more limiting approach to freedom of

[47] *Ibid.*
[48] *The Penal Code 1860* s 500.
[49] *The ICT (Amendment) Act 2013*s 57.

[50] Independent, The, *Section 57 to Be Scrapped* theindependentbd.com https://m.theindependentbd.com/post/125991.

[51] *Ibid.*
[52] *Ibid.*

expression in both its text and application. Demands for the DSA's abolition have increased as a result of this severe restriction on free speech. In response, the danger of using cyberspace unmonitored or unprotected has frequently been cited as a rationale for the regulation. In light of this, it's critical to pinpoint any issues with the Act.

Article 39 of the People's Republic of Bangladesh Constitution recognizes freedom of expression as a basic right. With the aforementioned assurance, however, it gives a large list of restricted grounds. This slew of restrictions on free expression has frequently been chastised for generating a slew of excessive exceptions to the general norm and for failing to meet international standards. Although the rule itself may require amendment, the explanation offered by the Constituent Assembly about its applicability might assist in avoiding unjustified restrictions on freedom. They contended that any limits on free expression must be fair and open to judicial scrutiny.Furthermore, the rules for applying the restriction reasons might be taken from international law, as Bangladesh has an obligation under international law to safeguard individual freedom of speech. In addition to these, comparative constitutional law principles of free expression can help guide a proper examination of the laws.

Apart from allowing for the arbitrary imposition of censorship, the Act also suffers from the fault of overcriminalization. The Act replicates, quite brutally, the old faults of criminalizing slander, sedition, and offending religious emotions, as done in the Penal Code 1860, a colonial remnant that is still in effect.

Again, Section 25 of the DSA makes it a crime to broadcast information with the goal of affecting the image or reputation of the nation or promoting confusion. This has no conceivable connection to the grounds of state security or other legally permissible restriction reasons. Penalties for remarks that merely harm the country's reputation or cause confusion are much too broad to be justified by any local or international norm. Furthermore, the provision's ambiguous and too broad phrasing might stifle statements on subjects of public concern.

Restriction should be implemented in a content-neutral way to minimize biases in free expression legislation. In other words, utterances may only be restricted if they incite impending violence or rioting. Section 31 of the Act goes into detail on utterances that incite animosity or disrupt community peace.

Therefore, Section 28 of the Act criminalizes utterances that offend religious emotions once more. Section 31's inclusion implies that Section 28 covers only prohibitions based on ideological content.Furthermore, it contradicts the notion of secularism, which is a key value and guide to the interpretation of the constitution.

Similarly, Section 21 prohibits propaganda or campaign against the liberation struggle, spirit of the liberation war, father of the country, national hymn, or national flag. This is, once again, a content-based limitation that is not just ambiguous and excessively broad. To make matters worse, these content-based prohibitions are subject to a disproportionate penalty and are classified as cognizable and non-bailable.

According to several media reports, more than 1500 complaints were filed under the DSA between January 1, 2020 and March 31, 2021.[53] In 2018, 925 cases were filed, 1189 cases in 2019, and 1128 cases in 2020.[54]The Centre for Governance Studies (CGS) was able to follow 890 cases with full information from January 2020 to February 2022 and undertake an analysis of the cases in a research.[55]

Judge As-SamsJoglul Hossain of the Cyber Tribunal of Dhaka recently rendered the first decision under this Act in the case of NusratJhahan Rafi v. State on November 29, 2019.[56]Former Sonagazi Police Station officer-in-charge Moazzem Hossain received an eight-year jail term with hard labor.[57] In this instance, NusratJahan Rafi, a madrasa student, was accused of having her testimony recorded and then disseminated online without her permission.[58]

---

[53]*Unending Nightmare: Impacts of Bangladesh's Digital Security Act 2018: CGS* Bay of Bengal Conversation https://cgs-bd.com/article/8915/Unending-Nightmare--Impacts-of-Bangladesh%27s-Digital-Security-Act-2018.

[54]*Ibid.*
[55]*Ibid.*

[56] June, TBS Report17 and TBS Report, *Bail Denied, Ex-OC Moazzem Sent to Jail* (June 18, 2019) The Business Standard https://www.tbsnews.net/bangladesh/crime/bail-denied-ex-oc-moazzem-sent-jail.

[57]*Ibid.*
[58]*Ibid.*

Additionally, he was fined Taka 10 lakh, failing which he must serve another six months in prison.[59]

Pornography Control Act (PCA) 2012

States throughout the world are implementing limitations or even outright prohibiting pornography to safeguard their inhabitants' futures after discovering the dangers it poses to them. Bangladesh, following the trend, has severely prohibited pornography under **the Pornography Control Act of 2012.**

Section 2 of the Pornography Control Act defines pornography as include nude or semi-naked video and still images.[60] Any content that is likely to arouse sexual arousal or desires is also included in the definition of pornography.

The 2012 Legislation states that users of the applications might easily be subject to section 8(1) of the act, which lists a sentence of up to 8 years in prison and a fine of up to TK 200,000 only for taking a photograph or video.[61]

Again, Section 8(3) states that a user who distributes such content over the internet or a mobile phone may face up to 5 years in jail and a fine up to the same amount as in the preceding section.[62]

The Statute contains a specific provision for child pornography, and under the Section 8(6) of this Act, any individual under the age of 18 is considered a kid, and any pornographic recording, photos with a child being filmed, would result in a 10-year jail sentence and a five-lakh-taka fine.[63] Another element of the Act is that it allows the Court to seek expert advice/assistance from IT specialists and allows the Investigation Officer to seize or examine any device, book, CD, or other material.NCMEC claims that Bangladesh's IP (Internet Protocol) address has been

[59] *Ibid.*
[60] *The Pornography Control Act 2012*s 2.
[61] *Ibid* s 8(1).
[62] *Ibid* s 8(3).
[63] *Ibid* s 8(6).

used to disseminate child pornography more than 550 000 times.[64] However, the website doesn't say how much of the child pornographic content is produced in Bangladesh.[65]

Section 11 of the Act stipulates that the Government may establish a Tribunal for the trial of offences under the Act which has not been established yet and also no Rules have been made by the Government as of now.Under this Act, any baseless or unfounded claim is punishable by up to 1 lac taka in fines and two years in prison.

The Bangladesh Telecommunication Act 2001

The Bangladesh Telecommunication Act of 2001 established a strong regulating body in the telecommunications industry, and section 53 of the Act grants the sector the ability to intercept communication systems to halt any undesirable cyber occurrences using telecommunications instruments in the nation.[66]

However, this is similarly comparable to the ICT Act in that it contains no further information regarding cybercrime. It contains an in-depth explanation of all forms of communication, including mobile, internet, telephone, and fax.

The Penal Code 1860

The Penal Code 1860 defines cybercrime as classic criminal behaviors like as theft, fraud, forgery, defamation, and mischief, all of which are punishable under our country's penal laws. The misuse of computers, as well as the internet or cyber, has given rise to a slew of new age crimes, which are handled by particular laws designed to punish these offences. For example, the ICT Act of 2006 identifies specific offences that are not covered by the Penal Code. Based on this law, I believe the Bangladesh Penal Code includes very few prohibitions concerning cyber-squatting. However, there is nothing in our penal law that addresses cybercrime such as hacking, internet time theft, and email bombing.

---

[64]Zayeef, Ahmed, *Bangladeshis Also Involved in Making and Sharing Child Pornography*Prothomalohttps://en.prothomalo.com/bangladesh/crime-and-law/bangladeshis-also-involved-in-making-and-sharing-child-pornography.

[65]*Ibid.*

[66]*The Bangladesh Telecommunication Act 2001*s 53.

Conclusion

Since then, state and federal governments have established a number of legislation to address the issue of illegal behaviors that happen online. The majority of these regulations didn't exist twenty-five years ago when cyberbullying, cyber stalking, wireless service theft, spamming, and illegal access were all commonplace.

Now that there are many laws in place, the challenge is in actually executing them. However, it may be claimed that our government is unable to manage cybercrime by using some Penal Code provisions. When the perpetrators of such crimes are never punished, it can be upsetting for the victims.It is required to pass a specific law that solely addresses cyber-related issues in order to curb cybercrime. Making a new legislation is highly challenging. Because of this, we have to go through a very difficult process if we want to establish a new legislation. First and foremost, we must develop a national strategy to address these sorts of crime. The government has to develop a strategy that unites everyone in combating the issue of cybercrime.Due to the fact that these Acts were not specifically created for cyber-related issues, I believe they are insufficient. Although some local police agencies have units dedicated only to fighting computer crimes, others are reluctant to look into and prosecute these kinds of offences.

However, the human mind's capacity is incomprehensible. Cybercrime cannot be completely eradicated from the internet. History demonstrates that no piece of legislation has ever been able to completely eradicate crime from the world. Making individuals aware of their rights and obligations to report crimes as a collective social responsibility is the only action that can be taken, along with tightening the laws' enforcement.

Chapter 4: Limitations of the existing Regulations& Necessary Recommendations

Introduction

As the old adage goes, "prevention is better than cure." It is preferable to start using cutting-edge technical measures to prevent various cybercrimes. Cybercrime is, however, seen in the context of the modern world‟s largest information freeway era. In the sphere of internet communication systems, intellectual criminals are already propagating crimes at an astounding rate. Criminal activity has evolved via the advent of technology in a variety of ways. Accordingly, laws ought to be created in a fashion that allows for strict enforcement of control over offences in the technical sphere.

However, neither domestically nor internationally do we have such strong legal protections.Even if there are certain norms and conventions, their implementation is hindered by technological issues such procedural complexity and a lack of an effective execution mechanism. Utilizing these advantages, criminals commit horrible crimes including hacking, sending harmful emails, disseminating offensive images, supporting cyber terrorism, as well as using intellectual property without permission. It endangers people's right to privacy and puts the security and tranquility of the world at risk.For the sake of maintaining both personal privacy and global safety and security, it is therefore imperative that such crimes be prevented. Ever other nation around the world has the ability to implement strong legislative restrictions that defend against cybercriminals inside the confines of their own borders. Bangladesh can also take the required initiatives to prevent cybercrimes from occurring online.

Here, in this chapter, the limitations of our existing rules and regulations will be briefly discussed. Moreover, there will also some recommendations be provided which may help to create a better cyber-space in future.

Limitations of Existing Laws

If we consider the current situation in our nation, we can easily see some shortcomings in the provisions currently in place regarding Bangladesh's cyber law, discussed below:

1) At the time of the ICT Act's adoption, section 39 stated that a Cyber Appellate Tribunal would be formed under section 82 of this Act.[67] However, there is no such tribunal in our nation, and appeals on cybercrime-related crimes are handled by the High Court Division.
2) Section 56 of the ICT Act, 2006 states that any appointment made by the government to serve as the presiding officer of a Cyber Appellate Tribunal is final and cannot be challenged in any way.[68] Additionally, no act or proceeding before a Cyber Appellate Tribunal may be challenged on the basis of a single flaw in the tribunal's constitution.[69] The abovementioned clause is inconvenient and is likely to be overturned by the courts since it violates the people' basic rights, which are guaranteed in Chapter III of Bangladesh's constitution.[70] The Government cannot assert immunity in its nomination to the CyberAppellate Tribunal since doing so would be against the letter and spirit of the Bangladeshi Constitution.
3) Section 57 of the ICT Act, as amended in 2013, makes it legal for law enforcement to detain anybody without a warrant and raises the maximum penalty for breaking the law to 14 years for violations of the Information and Communication Technology (ICT) Act of 2006.[71] This is one of the Act's fundamental flaws. The police in our nation are not trained, thus there is a possibility that the law would be erroneously implemented in various contexts.
4) Offenses under section 57 of the amended Act, crimes are non-bailable, which means bail is at the discretion of the court.[72]
5) A police officer not below the level of a Sub-Inspector of police is required to conduct any investigations under this Act, according to section 80 of the ICT Act, 2006,[73] are

[67] *The ICT Act 2006* s 82.
[68] *Ibid* s 56.
[69] *Ibid.*
[70] *The Constitution of the Peoples' Republic of Bangladesh.*
[71] *The ICT (Amendment) Act 2013* s 57.
[72] *Ibid*.
[73] *The ICT Act 2006* s 80.

given dictatorial powers under provision of the ICT Act, 2006for the purpose of investigating and preventing the conduct of a cybercrime.

6) Section 84 of the ICT Act does not specify how or in what specific ways any offence or violation committed outside of Bangladesh by anybody will be subject to its application.
7) Law enforcement authorities do not have extra territorial or multi-territorial jurisdiction under the ICTAct, although these powers are essentially useless. This is due to Bangladesh's lack of extradition agreements with many nations and reciprocity, unlike EU nations.
8) There was no relief when Section 57 of the ICT Act was repealed. In DSA, the government proposed even stricter rules. The DSA's expansive rules go well beyond the constitutionally and internationally recognized standards for allowable speech restrictions. The DSA has been used by the government to put an end to opposition and maintain its grasp on power. It is past time for the government to see reason and abolish the DSA's harmful provisions.
9) When someone is found guilty of making pornography without getting permission from the subject, they face penalties. According to Section 8 of the Pornography Control Act of 2012, he might be sentenced to seven years in jail.[74] Given the growth of child pornography, this Act provides specific measures for it, and a 10 year sentence for violating them is the result.[75]In reality, animation or other artificial processes are used to make child pornography. Because of this, it is challenging to blame anyone for this act.
10) It's absurd that judges and attorneys are more knowledgeable about the law than technology, especially internet technology. The investigators are similarly uninformed about technology and online behavior.
11) On the basis of internet-related issues or cyberspace, we do not have any specific ministries. However, it is a significant issue in our culture today. Similar to the natural offender, a large number of people are committing these offences quickly. As we don't have any guardians for this.

[74]*The Pornography Control Act 2012*s 8.
[75]*Ibid.*

Recommendations

There is no question that technical defenses are more effective than legal remedies in preventing high-tech crimes, but technology-advanced individuals have the ability to breach the security barrier at any time. So, in order to win the war against the aforementioned situations, legal and other associated remedies are required. The state has the option to start new initiatives in addition to the current solutions, following in the footsteps of other established high-tech nations. For this purpose the following recommendations may be proposed:

1) Bangladesh is a nation that values the rule of law. The Constitution is crucial in safeguarding and upholding both the state's and the general populace's rights and obligations. Constitutional protections against cybercrime may lead to a national mindset on cyber terrorism that may provide a noticeable improvement than any other administrative or legal remedy. Such measures may be introduced by an amendment to the constitution.

2)The government has to develop a strategy that unites everyone in combating the issue of cybercrime. Due to the fact that these Acts were not specifically created for cyber-related issues, I believe they are insufficient. We must abide by certain guidelines in order to enforce this set of regulations, such as- recognizing the issue as well as collaborations and shared accountability in the fight against individual crime

3)The ICT Act, 2006 stipulates that certain Acts must be amended as a first step in integrating the Internet into Bangladesh's legal system. Before the Bangladeshi legal system completely adopts and welcomes the internet, there is yet a long path to go. Especially, to satisfy public demand, Section 57 of the 2013 ICT Act amendment that allows law enforcement to detain anybody without a warrant and increases the maximum sentence for breaking the law to 14 years must be changed.

4) The Second, Third, and Fourth Schedules of the ICT Act shall be followed in order to alter the Evidence Act of 1872, the Bankers' Books Evidence Act of 1891, and the Bangladesh Bank Order of 1972. Additionally, several elements of the ICT Act of 2006 need to be changed.

5) The Copyright Act of 2000 is a significant step in the battle against specific types of cybercrime, including piracy, illegal media distribution of audio, video, and document content, intellectual property theft, etc. Copyrighted works' owners have the only authority to undertake

certain actions with regard to the work. Any individual who carries out one of these activities without being authorized may be held accountable for violating the copyright.

6)We will be protected from online crooks if our state controls a ministry; because this ministry is our protector. And in my opinion, once we have a protector, we can pass laws according to our wishes, and this department is made up of academics.

7) In order to guarantee the fairness of technical conflicts, judges, investigative officers, and attorneys should be taught and become experts in the field of technology.

8) The future belongs to the children of today. However, the foundation of our educational system is literature. Through their teachings, we must educate children about cyber-related concerns.

9) The majority of the time, everyday people fall prey to cyber dangers, and millions of machines are destroyed. This training is thus just as necessary as technological precautions. Therefore, it would be easier to battle cybercriminals and safeguard the virtual world if the general public was fully informed of the nature, potential effects, and cure for dangers. Hence, the government may play a significant role. The state should use various channels to educate the general public nationwide about this and other important topics. Additionally, NGOs and other groups can start a campaign in this area.

The chance of being a victim of cybercrime is rising in Bangladesh and its affects everyone. Without a question, the Internet provides thieves with unmatched chances. There are several things that may be done to guarantee a secure and reliable computer environment. It is essential to Bangladesh's national security as well as to each individual's feeling of wellbeing. In light of the most recent technological advancements, it is not simple or even conceivable to completely eradicate cybercrime from society, but it is quite possible to battle and monitor it. The initial and most important prerequisite for achieving the goal is for everyone to be informed of cybercrimes and the actions to be taken to avoid them.

Conclusion

We should come up with a general definition of cybercrime that would be applicable in every state, regardless of geography. It is important to unify the rules and regulations that govern criminal prosecution. No sovereign state has the authority to compel another sovereign state to bring a criminal case. As a result, the afflicted nation should step up and create its own laws, rules, and regulations for bringing those perpetrators to justice.

The ICT Act and the Pornography Control Act can help stop some minor breaches that are almost antiquated, but they are utter failures when it comes to the more severe offences like money laundering, credit card fraud, online theft, virtual child pornography, and online fraudulence through image manipulation.It has not participated into a worldwide cybercrime pact, nor has it improved existing laws, nor has it updated them as needed, nor has it efficiently applied them.

Cybercrime is similar to population growth in that it may be very difficult to regulate if it gets out of hand. It is past time for Bangladesh to reflect on this terrible menace and narrow the gap between international and domestic efforts in accordance.

Chapter 5: Conclusion

In the 21st century, we rely heavily on technology, and the Internet is one of the most efficient and convenient sources of communication and information. Not only does it provide quick access and time-saving features, it also protects against potential threats such as data theft, electronic fraud in the financial sector, identity theft, misuse of confidential information, hacking or cracking, cyber stalking, distribution, etc. are under dangerous threat to Pirated software, terrorism, credit card fraud, spamming, e-money laundering, ATM fraud, phishing. The scariest aspect is that all it takes to commit a cybercrime, which is a crime in itself, is knowledge, will, access to the Internet, and a computer. Computers are vulnerable and must be protected by regulation and protected from cybercriminals. Observing cybercrime and its phenomenon reveals that it, like any other crime, affects society as a whole. One of the best ways to thwart these scammers and protect your sensitive material is through an opaque security system that inspects all data accessed over the Internet using an integrated system of software and hardware.

Cybercrime is a term widely used to describe criminal activity that takes place on a computer or on the Internet.[76] The increasing dependence on computers in modern life is the root of evil known as cybercrime. In an age where computers control everything from microwaves and refrigerators to nuclear power plants, cybercrime takes on a very frightening nuance. Cybercrime is any crime committed using a computer or the Internet.

Although the term "cyber" is technically limited to internet crimes, it is more commonly used to refer to crimes committed using stand-alone computers. Agencies, law enforcement, and other stakeholders have serious concerns about the complexity of cybercrime attacks and the security of information available online. The increasing dependence on computers in modern life is the root of evil known as cybercrime.

Key loggers, powered voice recorders, retina imagers and other devices capable of tricking biometric frameworks into bypassing firewalls can be exploited by cybercriminals. The lack of

---

[76]Kaspersky, *What Is Cybercrime? How to Protect Yourself from Cybercrime* (September 30, 2022) www.kaspersky.com https://www.kaspersky.com/resource-center/threats/what-is-cybercrime.

evidence to bring criminals to justice has contributed to the rise of cybercrime. Besides, cybercrime against individuals includes a variety of crimes, such as sending child pornography and email harassment.Cyber harassment is when a criminal uses someone else's information to impersonate the victim. Criminals can commit crimes by using another person's cell phone number and computer-generated text messages. Various cyber laws are at work at every moment of the day: registering an email address, booking a train ticket online, e-commerce, withdrawing money from an ATM, paying utility bills, etc.

Computers are at the mercy of cybercriminals, and we need legal guidelines to keep them safe. The problem with protecting computer systems from unauthorized access is that there is always the possibility that something can go wrong, not because of human error, but because of amazing technology.

Law enforcement agencies are working to address this problem, but it is a pervasive problem, with many individuals falling victim to identity theft, hacking, and malicious software. The most effective preventative measure to curb this type of modern crime is modern legislation that addresses all aspects of cybercrime and can be adjusted to deal with emerging threats. Governments are enacting laws and raising public awareness to combat cybercrime. The Bangladesh Information and Communication Technology (ICT) Act, the Bangladesh Code of Criminal Procedure (1898) and the Bangladesh Code of Evidence (1872) form the basic general basis for all cybercrime related investigations. The usual safeguards provided in Bangladesh Information and when fundamental rights are threatened or violated.

Bangladesh's cybercrime occurs when criminals use technology to commit crimes such as hacking, sending malicious emails, distributing pornographic images, supporting cyber terrorism, and piracy of intellectual property. Laws should be designed to enable strict enforcement of administrative violations in the technical field. There are some shortcomings in the provisions currently in force regarding cyber law in Bangladesh.Firstly, establishment of Cyber Appellate Tribunal, in accordance with Section 82 of this Act[77]; however, there is no such appellate tribunal in our country, and appeals against cybercrime are handled by the High Court.

[77] *The ICT Act 2006*s 82.

Section 56 of the ICT Act 2006 states that the appointment made by the Government as Chairman of the Cyber Court of Appeal is final and cannot be challenged in any way.[78] Further, no act or proceeding in the Cyber Appellate Court can be challenged on the basis of a single error in the court's composition.[79] The government cannot claim immunity in its nomination to the Cyber Appeals Court as it is contrary to the letter and spirit of the Bangladesh Constitution.[80]

Again, section 57 of the ICT Act, amended in 2013, legalizes law enforcement to arrest people without a warrant and reduces the maximum sentence for violators of the 2006 Information and Communications Technology (ICT) Act from 7 years to 14 years pull up.[81] The original law permitted bail, but with the amendments, crimes under Section 57 of that law are not liable for bail. In other words, bail is at the discretion of the court. This Deputy Inspector has unlimited powers conferred on him by section 79 of the ICT Act 2006. This includes the power to enter a public place, search the place, and arrest without warrant any person found there who is reasonably believed to be responsible. Acts that violate this law.[82]

Moreover, under section 80 of the ICT Act 2006, police officers of the rank of Deputy Police Inspector and below are obliged to conduct investigations under the Act.[83] A police officer not below the rank of Sub Inspector or any other government official authorized in that regard by the Government for the purpose of investigating and preventing cybercriminal activity under the provisions of the ICT Act 2006, shall be given dictatorial powers.[84]

Furthermore, the ICT Law, 2006 contains a provision that anyone who breaks the law anywhere in the world, other than internet users in Bangladesh, will be punished under section 84.[85] However, this provision cannot be enforced at all without an international agreement specifically addressing cyber law. Section 84 of the ICT Law does not specify how or in what specific manner crimes or offenses committed by persons outside Bangladesh are applied. Law enforcement agencies do not have extraterritoriality or multilateral jurisdiction under ICT law,

[78] *Ibid* s 56.
[79] *Ibid.*
[80] *The Constitution of the Peoples' Republic of Bangladesh.*
[81] *The ICT (Amendment) Act 2013* s 57.
[82] *The ICT Act 2006*s 79.
[83] *Ibid* s 80.
[84] *Ibid.*
[85] *Ibid* s 84.

but these powers are essentially useless. There was no relief due to the repeal of section 57 of the ICT Act.

Prior to the enactment of this Act, the law applicable to cyber offences was the Penal code, 1860 which was enacted long back in 1860 when no one even thought of computer technology or cyber criminality. The enactment of the 2006 ICT Act necessitated the introduction of certain consequential amendments to certain provisions of the Criminal Code of 1860 and the Evidence Act of 1872 to meet the requirements of the new cyberspace crimes in this field.

Most developing countries such as Bangladesh have limited access to information and inadequate access to existing information due to inadequate existing infrastructure and inadequate education. The BTRC must play an important role in the fight against cybercrime, as people in the country support the prosecution of cybercriminals before they commit crimes such as mass bombings, resource smuggling and extortion. Without new and effective cybercrime laws over time, our government will not be able to control cybercrime.

There is a need to bring changes in the Information Technology Act to make it more effective to combat cybercrime. Bangladesh can also take necessary measures to prevent cybercrime from cyberspace. All countries of the world can enact effective legal regulations to protect against cybercrime within their borders. Current cyber-attack trends in Bangladesh call for immediate attention to maintain a robust and viable cyber security strategy.

Bangladesh is no exception, the problem of cybercrime is increasing due to the absence of advanced cyber security tools and the ignorance of people in handling technological devices. The country's laws do not seem to be enough to protect the country's cyberspace. International cooperation, improved technical know-how, acquisition of expertise, and campaigns to prepare people for how to deal with cyber security threats are some of the remedial aspects that countries can consider.

The state should promote the training of such professionals with significant national efforts. It is the time for Bangladesh to take measures to prevent and stop the threats posed by cybercrime. We must remember that innovation is a miracle like this, it changes its trends and ways every minute and we must be at our best to resist the correction.

BIBLIOGRAPHY

A. Articles

Singh, Talwant, *CYBER LAW & INFORMATION TECHNOLOGY*https://www.coursehero.com/file/22091388/cyberlaw/

Khan, SifatRahbar, *Cyber Law in Bangladesh through an International Lens* (April 29, 2022) The Business Standard https://www.tbsnews.net/thoughts/cyber-law-bangladesh-through-international-lens-411742

Khattab, Asser, *Bangladesh: Information and Communication Technology Act Draconian Assault on Free Expression* (November 20, 2013) International Commission of Jurists https://www.icj.org/bangladesh-information-and-communication-technology-act-draconian-assault-on-free-expression/

Unending Nightmare: Impacts of Bangladesh's Digital Security Act 2018: CGS Bay of Bengal Conversation https://cgs-bd.com/article/8915/Unending-Nightmare--Impacts-of-Bangladesh%27s-Digital-Security-Act-2018

B. Books

Nagpal, Rohas, *Evolution of Cyber Crimes* (November 22, 2017) Academia.edu https://www.academia.edu/35222024/Evolution_of_Cyber_Crimes_Rohas_Nagpal_Asian_School_of_Cyber_Laws

Goodman, Marc D and Susan W Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace* Full text of "The Emerging Consensus on Criminal Conduct in Cyberspace" https://archive.org/stream/TheEmergingConsensusOnCriminalConductInCyberspace/TheEmergingConsensusOnCriminalConductInCyberspace_djvu.txt

Karzon, Hafizul Rahman, *Theoretical and Applied Criminology* (Palal Prokashoni1st ed2004) 411

Chaubey, RK, *An Introduction to Cyber Crime and Cyber Laws* (Kamal Law House1st ed2009) 135.

Grabosky, Peter N, *Electronic Crime* (Pearson Prentice Hall1st ed2006) 2.

Brenner, Susan W, *Cybercrime Criminal Threats from Cyberspace (2010* (Praeger1st ed2010) 46.

Ahmed, Dr. Zulfiquar, *A Text Book on Cyber Law in Bangladesh* (National 6aw Book Company1st ed2009) 63-64

Hart, HLA, *The Concept of Law* (Oxford University Press Inc.2nd ed1994)

C. Journals

Cassim, Fawzia, *Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study*https://www.researchgate.net/publication/317904403_Formulating_specialised_Legislation_to_address_the_Growing_Spectre_of_Cybercrime_A_Comparative_Study

Hanif, Md. Abu, *Cybercrime and Cyber Law: Growth of the State Concerns and Initiatives in Bangladesh* (2018) http://www.aasmr.org/liss/Vol.5/Vol.5_No.2_2.pdf

Mia, Badsha, *Cybercrime and Its Impact in Bangladesh: A Quest for Necessary Legislation* (July 1, 2015) Academia.edu <https://www.academia.edu/13465468/CYBERCRIME_AND_ITS_IMPACT_IN_BANGLADESH_A_QUEST_FOR_NECESSARY_LEGISLATION>

D. Legislations

The Constitution of the Peoples' Republic of Bangladesh

The ICT Act 2006

The ICT (Amendment) Act 2013

The Digital Security Act 2018

The Bangladesh Telecommunication Act 2001

The Pornography Control Act 2012

The Penal Code 1860

E. Treaties

Universal Declaration of Human Rights United Nations https://www.un.org/en/about-us/universal-declaration-of-human-rights.

International Covenant on Civil and Political Rights OHCHR https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

F. Others

Cybercrime Cybercrime Definition https://techterms.com/definition/cybercrime

*ICT Brief Final Draft 20 November 2013*Scribdhttps://www.scribd.com/document/269184617/ICT-Brief-Final-Draft-20-November-2013.

*Bangladesh National Parliament - SAMSN*https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf.

বাংলাদেশ কম্পিউটার কাউন্সিল (বিবিধ) বাংলাদেশ কম্পিউটার কাউন্সিল (বিবিধ)- গণপ্রজাতন্ত্রীবাংলাদেশিরকারhttps://bcc.gov.bd/site/page/31309623-287a-4430-811b- d354f6d6cbeb/ICT-Act-2013

Kaspersky, *What Is Cybercrime? How to Protect Yourself from Cybercrime* (September 30, 2022) www.kaspersky.com https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Alam, Shahid, *Fathoming ICT (Amendment) Act, 2013* (March 7, 2015) The Daily Star https://www.thedailystar.net/fathoming-ict-amendment-act-2013-14762

Independent, The, *Section 57 to Be Scrapped* theindependentbd.com https://m.theindependentbd.com/post/125991

June, TBS Report17 and TBS Report, *Bail Denied, Ex-OC Moazzem Sent to Jail* (June 18, 2019) The Business Standard https://www.tbsnews.net/bangladesh/crime/bail-denied-ex-oc-moazzem-sent-jail

Zayeef, Ahmed, *Bangladeshis Also Involved in Making and Sharing Child Pornography*Prothomalohttps://en.prothomalo.com/bangladesh/crime-and-law/bangladeshis-also-involved-in-making-and-sharing-child-pornography

---