



Daffodil
International
University

“Cyber Regulations in Bangladesh: A Critical Legal Analysis”

A DISSERTATION

SUBMITTED TO THE DEPARTMENT OF LAW,

**DAFFODIL INTERNATIONAL UNIVERSITY, IN THE PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF**

MASTER OF LAWS (LL.M)

Submitted by: Mohammad Mazharul Islam

ID: 213-38-005, Batch: 36th

Program: LL.M.(Final), Department of Law

Daffodil International University

Supervised by: Mr. Mohammad Badruzzaman

Assistant Professor, Department of Law

Daffodil International University

Date of Submission: 30/09/2022

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF LAW,
DAFFODIL INTERNATIONAL UNIVERSITY, IN THE PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF LAWS (LL.M)

2021-2022

Date of Submission: 30/09/2022

Department of Law

Faculty of Humanities and Social Science

Daffodil International University

Dhaka, Bangladesh.

Letter of Transmittal

Mr. Mohammad Badruzzaman

Assistant Professor

Department of Law

Daffodil International University

Dear Sir,

It's a great pleasure for me that I have been able to make research on **“Cyber Regulations in Bangladesh: A Critical Legal Analysis”**. During concluding this research, I have given all of my best effort to form the useful research and by collecting all the relevant information from different sources that it can fulfill your expectation.

Therefore, I shall remain grateful to you if you pass through this research paper for your evaluation and I would be like that if any valuable recommendation is formed from your part in this matter.

I am always available for any further clarification of any part of this paper at your convenience.

Sincerely yours.

Name: Mohammad Mazharul Islam

ID: 213-38-005

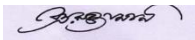
Program: LL.M.(Final), Batch-36th

Department of Law

Daffodil International University

Letter of Approval

This is to certify that the work is done “**Cyber Regulations in Bangladesh: A Critical Legal Analysis**” is a real work done by Md. Mazharul Islam, ID: 213-38-005, Batch: 36th, Department of Law, Daffodil International University, done under my supervision for the fulfillment of course requirements of Research Monograph (Law-812) and as the requirement for the degree of LL.M from the Department of law, Daffodil international University.



Mohammad Badruzzaman

Assistant Professor

Department of Law

Daffodil International University

Declaration

I, hereby, declare that the work, present in this research is performed by me under the supervision of Mr. Mohammad Badruzzaman (Assistant Professor, Department of Law, Daffodil International University). I also assure that this research or no part thereof is being submitted anywhere for the award of any degree.



Mohammad Mazharul Islam
(Candidate)

ACKNOWLEDGEMENT

I am grateful to almighty Allah for his mercies and grace. Thank you so much indeed for giving me sound health and mental strength throughout the entire period of this research.

This research work entitled “**Cyber Regulations in Bangladesh: A Critical Legal Analysis**” has been carried out at the Cybercrime related research of Department of Law, Daffodil International University with the support, encouragement, advice and guidance that I received from different people at different stages of this work. It is indeed my pleasure to record my indebtedness to them.

At the very first, I would like to express my earnest respect and thankfulness to my honorable supervisor Assistant Professor **Mr. Md. Badruzzaman**, for overall support, guidance and inspiration throughout the entire research work. Without your strong and efficient supervision, this work might have been very difficult.

I would also like to take the opportunity to express my sincere thanks to my departmental faculties for guiding and inspiring me throughout the entire period of this Master of Laws study. Your profound suggestions and recommendations have helped me to manage everything nicely during this degree study. I am grateful to all the teaching staff of Daffodil International University. My special thanks go to my Best Friend Eshita Islam for her endless support, excellent inspiration and nice company during busiest days of this research work. Thank you so much indeed. I am happy and really lucky to have you beside me.

Last but not the least; I do record my heartiest indebtedness to **Daffodil International University** for providing me the opportunity to complete this research work.

**This Thesis Is Dedicated
To
My Mother and Eshita Islam**

ABSTRACT

This research is predicated on cybercrime only. The method of combating cybercrime is described here and also the implementations of laws are shown in it. This thesis is completely supported laws of our country. It also focuses the lacking of our laws and the way to unravel this problem; it also described. A way to combat cybercrime and by which way; it also mentioned here. Describe the combating system, which is mentioned in our Acts. What's the scenario of our country; also shown during this. Bangladesh isn't capable to combat it now; it's proved during this research and also the way of overcome from this is often also mentioned. We've no any laws to combating cybercrime and why it's urgent to create it; also elaborate during this research.

TABLE OF CONTENTS

Letter of Transmittal.....	i
Letter of Approval.....	ii
Declaration.....	iii
Acknowledgement.....	iv
Dedication.....	v
Abstract.....	vi

S.L.	CONTENTS	PAGE NO.
------	----------	----------

CHAPTER - 1

PRELIMINARY

1.1.	Introduction	1
1.2.	Statement of the Problem.....	1-2
1.3.	Literature Review	3
1.4.	Significance of the Research.....	4
1.5.	Objectives of the Research.....	4
1.6.	Research Methodology.....	5
1.7.	Modes and Sources of Data Collection.....	5
1.8.	Limitation and Scope of the Study.....	6
1.9.	Conclusion.....	6

CHAPTER - 2
CYBER LAWS IN BANGLADESH

2.1.	Introduction.....	7
2.2.	Information and Communication Technology Act, 2006.....	7
2.3.	This Act declared the following actions to constitute Cybercrimes.....	8
2.4.	Limitations of the aforementioned Act.....	9
2.5.	Digital Nirapotta Ain 2018.....	9-10
2.6.	Cyber Tribunal.....	11
2.7.	Cyber Appellate Tribunal.....	12
2.8.	Pornography Act 2012 and Child Pornography.....	12
2.9.	Penal Code 1860.....	13
2.10.	Bangladesh Telecommunication Act 2001.....	14

CHAPTER - 3
FORUM FOR REDRESS

3.1.	Specific Body to Handle.....	15
3.2.	Investigative Authority in Cybercrime.....	15-16
3.3.	Trial Procedure.....	17
3.4.	Execution/Remedy.....	18-20

CHAPTER - 4

CHALLENGES FOR IMPLEMENTATION OR COMBATING CYBER CRIME

4.1.	National Plan.....	21
4.1.1.	Recognizing the issue.....	21
4.1.2.	Partnerships and shared responsibility; individual crime.....	21
4.1.3.	A prevention-centric approach.....	21
4.1.4.	Balancing security freedom and privacy.....	22
4.2.	Law Makers on the Basis of Cyber.....	22
4.3.	Law Ministry on the Basis of Cyber.....	22
4.4.	Public Awareness about Cybercrime.....	22
4.5.	Internet Based Education.....	22
4.6.	Digital Security.....	23
4.7.	Investigational Power and Investigational System.....	23

CHAPTER - 5

CONCLUSION: FINDINGS AND RECOMMENDATIONS

5.1.	Introduction.....	24
5.2.	Criticisms.....	24
5.3.	Findings.....	25
5.4.	Recommendations.....	26
5.5.	Conclusion.....	26

BIBLIOGRAPHY.....	27-28
-------------------	-------

Cyber Regulations in Bangladesh: A Critical Legal Analysis

CHAPTER - 1

PRELIMINARY

1.1. Introduction

In Bangladesh, crime involving technology and the internet is increasing. It is a major issue in Bangladesh. In the field of data technology, an emerging threat has already been identified. Cybercrime is commonly defined as any criminal activity that jeopardizes information technology, such as unauthorized access.¹ Cybercrime is defined as "offenses committed against a private or group of people with a criminal motive to intentionally damage the victim's reputation or cause the victim physical or mental harm or loss directly or indirectly, and also sometimes guaranteed to suicide using modern telecommunication networks such as the internet (chat rooms, emails, notice boards or groups, social media, by sending spam) and transportable (SMS/MMS)."² Cybercrime is rising quickly in Bangladesh since there are no explicit laws based on the internet. There is no stopping it. We can consider the safe house of the internet if we create a clear law and a separate organization with expertise in this.

1.2. Statement of the Problem

Bangladesh has experienced a technology revolution despite being a third-world nation. Teenagers in Bangladesh can get to computers and other technology relatively quickly. They consequently have ample opportunities to hack. In Bangladesh, hacking is already a serious issue. Not just teenagers, but even members of the mainstream media frequently break into computers and leak sensitive data.³ On February 15, 2012, a group of alleged Bangladeshi hackers known as the "Black Hat Hackers" hacked more than 25000 Indian websites, including important sites such as the

¹ Pavan Duggal, 'Causes Of Cyber' (2016) 3 International Journal of Computer Science and Information Security.

² Ripon Kumar Biswas, 'Cybercrimes Need More Attention' <<http://www.cybercrimeslaw.net>> accessed 02 September 2022.

³ 'BDLD - A Leading Law Magazine/Journal In Bangladesh' (Bangladesh Law Digest (BDLD), 2022) <<http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/>> accessed 2 September 2022.

Border Security Forces website (BSF).⁴ We can bring up the Ramu Violence in Cox's Bazar in 2012. Crowds of angry Muslims attacked Buddhist shrines and a home in Bangladesh, torching some of them in protest after a photo of a partially burned Quran was posted on Facebook.⁵ However, the attacks were meticulously planned and executed. As a result, it is clear that Bangladesh is not immune to cybercrime.

On March 11, 2016, \$101 million in Bangladesh Bank (BB) funds were stolen, with \$81 million wired to two banks in the Philippines. According to the BB, the remaining \$20 million was transferred to a bank in Sri Lanka in favor of an NGO whose account was opened just a month ago.⁶ Additionally, money was stolen from numerous banks using ATM skimmers. New types of cybercrime are occurring every day, and if they are not stopped, the situation with law and order will get worse.⁷ It's crucial to create a body if you want to create a safe cyberspace for your home. who are knowledgeable with technology-related concerns such as the internet and other similar topics. To persuade the government to construct such safety house, this research is crucial. We can easily catch the offender if we create a body solely dedicated to the protection of this industry and if we maintain a strategy along the lines of "everyone who wants to access the internet must maintain a rule." The rule is that everyone must register for internet access using their national identification number or birth certificate number before they can use it. Otherwise, they will not. No one can create a duplicate ID number in any site this way (as like social media sector, official sector, government sector etc.). Furthermore, all access is recorded and reserved. Some other rules are also important, such as when someone accesses a red-flagged page, a notification is sent to the security house, and the agency can easily arrest the offender, after which we can easily apply the other Acts to prevent cybercrime.

As a result, I believe it is crucial to conduct research in this area.

⁴ 'Bangladeshis Hack 20,000 Indian Websites' (Gadgets 360, 2012) <<http://gadgets.ndtv.com/internet/news/bangladeshis-hack-20000-indian-websites-224516>> accessed 2 September 2022.

⁵ Farid Ahmed, 'Bangladesh Muslims Torch Buddhist Shrines, Police Say | CNN' (CNN, 2012) <<http://edition.cnn.com/2012/09/30/world/asia/bangladesh-muslim-buddhist-violence/>> accessed 1 September 2022.

⁶ 'Hackers Bugged BB System In Jan' (The Daily Star, 2016) <<http://www.thedailystar.net/frontpage/hackers-bugged-bb-system-jan-789511>> accessed 1 September 2022.

⁷ 'BDLD - A Leading Law Magazine/Journal In Bangladesh' (Bangladesh Law Digest (BDLD), 2016) <<http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/>> accessed 3 September 2022.

1.3. Literature Review

This research which based on, “**Cyber Regulations in Bangladesh: A Critical Legal Analysis**”.

Many people define cybercrime and control by their personal experiences. What constitutes cybercrime is often defined. However, I believe that some materials—namely, "Has there been any specific body to control it? Can we regulate cybercrime with the laws in place today? On the basis of this query, I believe their definition is unclear. Nowadays, a lot of lawsuits are filled based on cybercrime. Mr. **Sufi Faruq Ibne Abubakar**, wrote about this subject in his article. He said that, *“The concept of a Digital Bangladesh is welcomed by the IT professionals and the general mass. To fuel this notion the government must give due importance to the matter of cybercrime. Otherwise, like many other positive initiatives this will fall on its face. It is a matter of hope that the “National Information and Information Technology Guidelines 2009” has included Cybercrime as an agenda. To make this a success the Ministry of Information Technology, along with the IT professionals and the media must come forward.”*⁸ In Bangladesh, we have a law based on cybercrime called the ICT Act 2006 and the Digital Nirapotta Ain-2008. However, these are insufficient to reduce cybercrime. We need a body that can control it. Our laws contain numerous loopholes. The internet has become an integral part of the lives of all educated people around the world. However, I disagree with him in that today's internet users include both educated and illiterate individuals. As a result, they will not be able to determine which website is malicious and engaging in illegal activities. However, they are not well-versed in internet etiquette. On the flip hand, some evil individuals who are both educated and illiterate voluntarily engaged in such illicit actions on the internet. Today, anyone can use the internet relatively readily, but if we had a body to regulate the sector and set strict guidelines for usage, we might lessen the scope of criminal activity.

⁸ <<http://sufi-faruq.com/en/combating-cybercrime-a-bangladeshi-perspective-2/>>

1.4. Significance of the Research

Hacking of the RAB website, ATM card skimming, the heist of the Bangladesh Bank, and terrorist activities on social media are just a few examples of cybercrime. Furthermore, cyberbullying is becoming a major concern for parents regarding their children's internet use, as the majority of students in Bangladesh have been bullied or disturbed online, or have been bullied by the same person both online and offline. Furthermore, cybercrime is becoming a threat to the government. Cyber criminals are almost unafraid to commit such crimes due to a lack of necessary legislation to combat such crime. There are several anti-cybercrime provisions in the Information and Communication Technology Act of 2006 and the ICT (Amendment) Act of 2013. However, this act on information and communication technology is not the concrete one. There is a chance to become safe after committing crimes by enacting this act. Given these facts, a comprehensive Cybercrime Protection Act should be enacted. This research work incorporates the most recent trends and issues of cybercrime in Bangladesh, with a particular emphasis on personal life, workplace, and policy making bodies or thinkers. This work, I believe, will benefit all relevant stakeholders, particularly policymakers.

1.5. Objectives of the Research

The main goals of this research is:

- To discover the existing problems of cyber law in our country in order to control cybercrime;

Ancillary Objectives

- To examine the cyber issues of Bangladesh and examine legal protection relating to cybercrime;
- To discuss the forms of cybercrime and discuss intervention strategies that will help to end cybercrime.

1.6. Research Methodology

It is an exploratory piece of research. It combines qualitative and quantitative research. The victims' stories and cases should be investigated to learn more about their online social lives, fears of becoming a victim of cybercrime, and the status and factors that contribute to victimization. Various methods of data analysis, including frequency distribution, causality, factor analysis, and other statistical instruments of analysis, shall be used to construct a logical framework. The laws and practices in this area will be looked at and evaluated in the context of this study. Numerous research techniques would be utilized to give the study its final form, including:

- an analysis of related secondary sources and instruments on cybercrime;
- an examination of the constitutional guarantees regarding the right to legal protection and other relevant provisions in the Bangladesh Constitution;
- an analysis of statutory law and case law relating to cybercrime in Bangladesh;
- a review of relevant public records, available statistical data, and annual reports of various NGOs; case studies of specific incidents relating to cybercrime; and
- data collection and analysis.

The secondary literature, which consists of books, journals, electronic resources, case law, statutes, and legal precedent, will be the foundation for the discussion of the conceptual questions.

1.7. Modes and Sources of Data Collection

The research will use both primary and secondary data. As a primary data collection technique, national statutes and all types of verified news portals would be used. The researcher will visit the individuals and send the questionnaire via email. Secondary data will be gathered from the topic's literature as well as Annual Reports of major non-governmental organizations. Furthermore, data will be gathered from the websites of various national and international organizations. The collected data will be classified, analyzed, and tabulated in accordance with the study's objectives and variables. The final chapter will draw an overall conclusion.

1.8. Limitation and Scope of the Study

The study area is within Bangladesh because the researcher will find it easier to collect information and data there because it is his workplace. It should be noted that if there is a prominent or significant case, this study will specifically focus on women, children, or juvenile victims and offenders. The research will last one month. Due to time and financial constraints, the study is limited in terms of time and location.

Although the term "cybercrime" is more properly limited to criminal activity in which a computer or network is a necessary part of the crime, it is also sometimes used to include traditional crimes such as fraud, theft, blackmail, and so on, in which computers or networks are used. Cybercrime has grown in importance as the use of computers has increased. Fighting cybercrime in Bangladesh is difficult due to the lack of a strong legal framework. "Existing laws alone are insufficient." To meet the growing challenges in cyberspace, existing laws must be amended."⁹

1.9. Conclusion

Cybercrime is clearly the most recent form of crime that is extremely difficult to combat. However, this difficulty should not prevent us from taking adequate measures against cybercriminals. It is past time to mark off the upcoming cyber threats to Bangladesh and other related issues. The government must maintain constant vigilance and improve counter-measures. Ordinary people should exercise caution when using computer systems and online services.

⁹ 'BDLD - A Leading Law Magazine/Journal In Bangladesh' (Bangladesh Law Digest (BDLD), 2015) <<http://www.bdldigest.org/cyber-crime-a-new-menace-in-modern-era/>> accessed 1 September 2022.

CHAPTER - 2

CYBER LAWS IN BANGLADESH

2.1. Introduction

Crime The ICT Act, 2006 was passed with the intention of promoting e-commerce and the development of information technology. It contains provisions with a maximum penalty of 10 years imprisonment, a fine of up to 10 million Taka, or both. However, our Parliament recently amended the ICT Act 2006, increasing the penalties for cybercrime to a minimum of 7 years imprisonment and a maximum of 14 years, or a fine of Tk. 1 core, or both. The Information and Communication Technology (ICT) Act of 2006 went into effect on October 8, 2006. The government then amended the Act in 2008, 2009 and 2013. In order to improve the implementation of the Act, the government issued Information Technology (Certificate Authority) rules in 2010. These laws, however, are insufficient. To meet the growing challenges in cyberspace, existing laws such as the Penal Code 1860, the Evidence Act 1872, the Contract Act 1872, and others must be amended. It is hoped that these Acts will be amended in response to changing circumstances.

2.2. Information and Communication Technology Act, 2006

The ICT Act, 2006 contains some clauses that outline the consequences for numerous offenses relating to cyberspace. For example, section 54 (1) of this Act lists the cyberspace-related offenses. According to section 54(2), "Anyone who commits offenses under sub-section (1) of this section shall be punished with imprisonment for a term that may extend to ten years, with a fine that may extend to taka ten lakhs, or with both." Additionally, Section 56, which states that "If any person—

(a) 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 that destroys, deletes, or alters any information residing in a computer resource, or diminishes its value or utility, or adversely affects it by any means.

(b) damage caused by unauthorized access to a computer, computer network, or electronic system that does not belong to him shall be considered a hacking offense;

(c) whoever commits a hacking offense under sub-section (1) of this section is punishable by imprisonment for a term of up to ten years, a fine of up to taka one crore, or both."

We can see that the issue of cybercrimes has received legal attention, and there are some tight regulations surrounding it.

2.3. This Act declared the following actions to constitute Cybercrimes:

- Any data, database, or file that has been copied, extracted, or downloaded without authorization
- Virus introduction
- Computer system and computer network damage and disruption
- Denial of authorized person access to computer
- Providing assistance in order to commit crime
- Computer system hacking
- Computer source documents manipulation.
- Electronic forgery with the intent to defraud and harm someone's reputation
- Using a falsified electronic record
- Publishing a digital signature certificate with malicious intent
- Computer, network, etc. confiscation
- The electronic publication of pornographic material
- Making false statements and omitting important information to obtain a digital signature certificate
- Privacy and confidentiality violations
- Publication of a forged digital signature certificate.

2.4. Limitations of the aforementioned Act:

Critics draw attention to the fact that the aforementioned Act still has the following specific limitations.

1. Different intellectual property rights, such as copy rights, trade-mark rights, and patent rights of e-information and data, are not addressed by the Act.
2. The law's implementation has a significant impact on Bangladesh's m- and e-commerce. But it keeps quiet about any transactions that are paid for electronically.
3. The law was initially intended to cover crimes committed anywhere in the world, but no one is sure how this would actually work out.
4. Western nations have developed measures in their cyber laws to combat spamming since it has become a threat. However, our Act does not contain any anti-spam provisions.
5. The main issue that directly affects the online world is domain names. However, the definition of "domain name" and the associated rights and obligations are not included in the ICT Act, 2006.
6. Mobile phone-related crimes are not covered by the Act.
7. This law recognized e-mails as evidence, in contrast to the country's Evidence Act, which does not recognize e-mails as evidence.

To ensure a peaceful society free from cybercrime, we hope that our government would take the appropriate steps to address the issues.

2.5. Digital Nirapotta Ain 2018

This Act, an updated version of the nation's cyber-protection law, will take the place of several contentious elements of cyber-security laws, such as Section 57 of the ICT Act 2006. The Digital Nirapotta Ain 2018 has a few fundamental aspects, such as: it acknowledges and defines e-commerce and e-transactions. Section 4 of the Act demonstrates the Act's jurisdiction, which extends both within and beyond the borders of Bangladesh.¹⁰ Section 5 refers to the establishment of a Digital Security Agency, which is responsible for monitoring and supervising digital

¹⁰ Section 4 of Digital Nirapotta Ain 2018

information and communications channels, including mobile phones, in order to combat cybercrime. This section also introduces the Bangladesh Cyber Emergency Incident Response Team and the Digital Forensic Lab (Bangladesh- CERT).¹¹ The power of the DG of the Digital Security Agency is demonstrated in Section 13 of the Act, where the DG may order a communication restriction in extraordinary circumstances (security breach or national-international threat) to any person or service provider.¹² In that instance, the person or service provider must make it possible for the Computer or source to be intercepted, watched over, and decrypted. On the basis of Section 15, it states that the Act uses examples of hacking, impersonation, privacy violations, and other cybercrimes.¹³ According to Section 15(5) of the Act, any disparaging remarks, campaigns, or propaganda in electronic media made by an individual, organization, or foreign national against the liberation struggle, the father of the nation Bangabandhu Sheikh Mujibur Rahman, or any matter that has been adjudicated by a court, constitutes a violation of the Act.¹⁴ The Act's Provision 36 states that the violation covered by this section is both cognizable and non-billable.¹⁵ Section 16 depicts the punishment for offenses under Section 15 (cybercrimes, propaganda against the Liberation War or Bangabandhu), ranging from 3 years to life imprisonment and/or a fine of 10 million taka.¹⁶ Anyone who assists or abets the commission of any offense under the Act is considered to have committed a similar offense under Section 21 and is subject to the same punishment.¹⁷ The trial under Digital Nirapotta Ain 2018 will take place before the same Cyber Tribunal that was set up under the ICT Act of 2006, and the tribunal's procedures will be similar in that the trial must be finished in 180 days.

I will make sure to clearly explain how Section 2 of the Digital Nirapotta Ain 2018 defines terms like "lawful access," "illegal access," "critical information infrastructure," "e-transaction," "e-payment," "data corruption," "data," "program," "digital network," "subscriber information," "traffic data," "electronic forgery," "digital pornography," "digital child pornography," etc.¹⁸ But this Act makes no mention of how it will be stored. Here, 30% of the laws are new, but at least

¹¹ Section 5 of Digital Nirapotta Ain 2018

¹² Section 13 of Digital Nirapotta Ain 2018

¹³ Section 15 of Digital Nirapotta Ain 2018

¹⁴ Section 15(5) of Digital Nirapotta Ain 2018

¹⁵ Section 36 of Digital Nirapotta Ain 2018

¹⁶ Section 16 of Digital Nirapotta Ain 2018

¹⁷ Section 21 of Digital Nirapotta Ain 2018

¹⁸ Section 2 of Digital Nirapotta Ain 2018

70% of them are just repeats of older laws like the ICT Act, the Penal Code, and the Code of Criminal Procedure. In this Act, it is not explicitly stated where to get officers to maintain the sector. There are still certain gaps in this area, such as the Police's ability to investigate and act as this sector, but I believe that an IT sector specialist should be hired to work for a law enforcement agency in order to regulate this industry. In the case of Nusrat Jhahan Rafi v. State, Judge Ash Sams Joglul Hossain of the Cyber Tribunal of Dhaka rendered the first decision under this Act on November 29, 2019. Former Sonagazi Police Station officer-in-charge Moazzem Hossain received a sentence of eight years rigorous imprisonment. In this case, the defendant was charged with filming madrasa student Nusrat Jahan Rafi's statement and distributing the video clip on social media without her permission. He was also fined Tk 10 lakh, failing which he will be imprisoned for another six months.¹⁹

2.6. Cyber Tribunal

According to section 68 of the Information and Communication Technology Act, 2006, the government shall establish one or more cyber tribunals for the swift and efficient resolution of disputes under this Act. The Government will decide the tribunal's local jurisdiction, and the tribunal will only try offenses covered by this Act. The Government shall appoint a Sessions Judge or Additional Sessions Judge as a judge of the Cyber Tribunal after consulting with the Supreme Court. A case will be heard by the cyber tribunal –

a) based on a complaint made by a controller designated under this Act or by any other person authorized by the controller, or b) based on the report of a police officer not below the level of sub-inspector.

As long as it is consistent, chapter 23 of the Criminal Procedure Code, 1893 (Trial Procedure by the Court of Sessions) will be followed in the cyber tribunal's trial process. The court may conduct an absentia trial if the accused flees. In order for the accused to appear on a particular date, the tribunal in this case must publish an order in two Bangla publications. The Cyber Tribunal shall apply the provisions of the Criminal Procedure Code and shall have the same authority as a Sessions Court in its original jurisdiction. The case will be handled on behalf of the government by the public prosecutor. The tribunal must complete the trial within six months of the charge

¹⁹ The Daily Star, Saturday, November 30, 2019

being filed. This time frame could be extended for three months. The Tribunal shall issue its decision within ten days of the conclusion of the trial, which may be postponed for ten days.

2.7. Cyber Appellate Tribunal

One or more cyber appellate tribunals shall be established by the government. The appeal tribunal will consist of a chairman and two other members who will be chosen by the government. He must be a judge of the Supreme Court currently, have served as a judge of the Supreme Court in the past, or be qualified to serve in that capacity in order to be selected as head of the Cyber Appellate Tribunal. The other member of the tribunal must have knowledge and expertise in information and communication technologies, and one of the two members must be a retired District Judge or currently serving in the judicial service. They will serve for three to five years. No original jurisdiction shall exist for the Cyber Appellate Tribunal. Only in relevant instances will it hear and decide appeals from the Cyber Tribunal's and Sessions Court's rulings. The appellate tribunal's decision is final, and it has the authority to overturn the first tribunal's order and judgment as well as change or repeal it. The Supreme Court's High Court Division appellate procedure will be followed by the appellate body. Until a cyber appellate panel is constituted, the High Court Division may hear an appeal.

2.8. Pornography Act 2012 and Child Pornography

To safeguard women, children, and adults against sexual harassment, blackmail, and other forms of exploitation, as well as to stop the widespread distribution of sexually explicit videos, MMS, and pictures via mobile devices and other channels—not to mention the internet. This Act became a law on March 8, 2012. Give an explanation of what pornography is in section 2.²⁰ Section 5 describes the investigation procedure, and the other sections describe the punishment procedure and other such issues. However, there are no words that are clearly related to cyber activities.²¹ However, there are no additional special laws or regulations to stop child cybercrime or child pornography in general. I believe that the Anti-Pornography Act (2012) was passed by the Bangladeshi government to limit the sharing and production of pornographic material by individuals since it has devastating effects on both the individual engaged and society as a whole.

²⁰ Section 2 of Pornography Act 2012

²¹ Section 5 of Pornography Act 2012

According to Section 4, pornography cannot be produced, stored, distributed, carried around, bought, sold, held, or shown.²² Section 7- An investigation of any violation of this Act or any technical expert certified by the competent authority in the course of the violation has been committed to a government, autonomous, semi-autonomous organization in charge of the technical department, and private individuals or any person or organization. The opinions of experts from the comments received shall be treated as those of the technical competent institutions in charge of the accredited individuals, and they may be used as evidence in court.²³ Section 10- Any offense committed in violation of this Act shall be cognizable and non-billable.²⁴ Section 11- Any offense committed under this Act must follow the procedure outlined in the Code of Criminal Procedure. Provided, however, that the Government may appoint, by notification in the official Gazette, a special court or tribunal to hear crimes committed under this Act.²⁵ However, it is insufficient for combating cybercrime. Because this Act is only concerned with pornography.

2.9. Penal Code 1860

The Penal Code 1860 defines cybercrime as traditional criminal activities such as theft, fraud, forgery, defamation, and mischief, all of which are punishable under our country's penal laws. Abuse of computers, the internet, and cyberspace has also given rise to a wide range of new age crimes, which are handled by particular laws passed to punish these crimes. For instance, the ICT Act of 2006 identifies specific offenses that are not covered by the Penal Code. Based on this statute, I believe that there are not many prohibitions against cyber-squatting in Bangladesh's Penal Code. However, our penal code says nothing about cybercrime like hacking, internet time theft, or email bombing. Therefore, it can be claimed that our government is unable to manage cybercrime by applying some penal code provisions. It is required to pass a special law that only addresses cyber-related issues in order to curb cybercrime.

²² Section 4 of Pornography Act 2012

²³ Section 7 of Pornography Act 2012.

²⁴ Section 10 of Pornography Act 2012.

²⁵ Section 11 of Pornography Act 2012.

2.10. Bangladesh Telecommunication Act 2001

The Bangladesh Telecommunication Act of 2001 established a powerful regulatory authority in the telecommunications sector, and Section 53 of the Act gives the sector ample power to intercept communication systems in order to prevent any unwanted cyber incidents with the use of telecommunication tools in the country.²⁶ 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.

²⁶ Section 53 of Bangladesh Telecommunication Act 2001.

CHAPTER - 3

FORUM FOR REDRESS

3.1. Specific Body to Handle

According to our legal system, there is no specific forum for dealing with it. The actual definition of a forum is an independent body that only performs for a specific sector. As I've said before, we need experts to handle any situation. But there are no expert law enforcement agencies in the cyber sector. To handle these related matters, they must have extensive knowledge of cyber issues. But, do they know much about technical issues? They haven't, I guess. Because according to a figure I have, only 3,650,000 out of 16,36,54,860 individuals currently utilize the internet, and this ratio was established between 2007 and today.²⁷ The question is, how many law enforcement agencies are experts in it out of this group? I estimate that 2% of the 3,650,000 people and 8% of this are merely online. So how can it be claimed that we have a forum to fight cybercrime? Therefore, I claim that we haven't. Is there a certain organization that handles it? Along with the Police, RAB, etc. No one who is knowledgeable in the field of cyber exists here. Many cases are still pending due to the deficiency. The investigation process for cybercrime is different from that in other cases. Another issue is that Bangladesh does not have any specific laws that address the forum. We may also have the system to deal with it.

3.2. Investigative Authority in Cybercrime

According to our country's laws, it is crystal clear that a police officer who does not hold the level of sub-inspector is not permitted to look into any cases of cybercrime. On the other hand, a few other organizations including CID, DB, SB, etc. also look into that topic. However, there is a certain organization here called the controller that is empowered to look into such an issue.²⁸ Without limiting the provisions of section 54 of the ICT Act, the Controller or any person authorized by him may access any computer system for the purpose of searching or causing a search to be made in order to obtain any information or data contained in or accessible to such

²⁷ <<http://tech.firstpost.com/news-analysis/5-things-all-broadband-users-must-know-81724.html>–[last visited on 07th August,2022].>

²⁸ DR. Zulfiqar Ahmed, A Text Book On Cyber Law In Bangladesh (1st edn, National Law Book Company 2012).

computer system if he has reasonable cause to suspect that any violation of the Act or rules and regulations made there under has been committed.²⁹ If we focus on other criminal matters or natural crimes, we'll notice that the police frequently handle investigations into both cyber-related issues and other criminal topics. But now the question is that Is he knowledgeable about those highly sought-after things? No, I believe. Because no one can be an expert in every field, whether it be economics, murder, or cyber, it is impossible for anybody to know everything about everything. However, how does the current investigation procedure on cyber-related matters work? It is open to investigation by any sub inspector. Is it relatively easy? No, since he investigates it if someone doesn't fully understand the situation. What will happen after that? His ignorance of this particular topic renders all investigations useless. Because of their familiarity with and knowledge of this particular subject, we readily accept it. But in the end, it is obvious that the investigation process is the same as that in other criminal instances. How can we now look into it?

- By creating a body for cyber intelligence and analysis.
- By setting up a lab for cyber-forensics.
- By establishing a center for research.
- By constructing a training facility to wage war on them.
- By creating an information warehouse.
- By creating an independent body.
- By creating an enforcement body to look into those matters.

Investigating in this area may be quite challenging, but by continuing in the right direction, the problem will be resolved. We don't receive any appropriate institutional education on it. Because of this, it seems like a challenging situation. We must quickly construct it. Knowing the internet protocol to identify the person who committed the crime can help us find the perpetrator. By identifying his IP address, we must quickly learn his address or all other relevant information before beginning the investigation.

²⁹ Section 30(1) of The Information Technology Act, 2006.

3.3. Trial Procedure

Any cybercrimes will be tried in accordance with specific legislation, such as the ICT Act of 2006, the Digital Security Act of 2012, the Penal Code, and the CrPC as well. If we look at the punishments, they are the same: a minimum of seven years and a maximum of fourteen years of imprisonment, as well as a fine. maximum fine of one million taka. Sections 54, 56, 57, and 61 of the ICT Act of 2006 deals with cybercrime and mention it. It was also stated plainly here that these crimes are not punishable by law and are not cognizable offenses. By using section 54 of the CrPC, police enforcement is given the authority to detain anyone who is accused of breaking the law without a warrant.³⁰ The authority established a special tribunal for the prosecution of cybercrimes on the basis of this Act. Government may establish one or more tribunals by filing a gazette. These tribunals will be run under Supreme Court supervision and will include session judges as well as any additional sessions that are cyber tribunals. Those who are sub inspectors and any officers who are given authority by them at the very least have the ability to conduct investigations. Additionally, no special tribunal may accept any matter on his tribunal without the officer's prior authorization. Judges must adhere to CrPC chapter 23 during trials. No court can halt a case unless it serves the interests of justice. If a criminal escapes from detention, the tribunal will post news to summon him to court on the specified date in the newspaper. If he doesn't show up after that, the court will begin trial in absentia. However, this rule will not be followed if he only appears once. CrPC will be followed. I can tell that the legal system and trial procedure here are identical to those used in other cases. However, in my opinion, we ought to bring in an expert to testify on this cyber topic. The judicial system will suffer without it. Without having the necessary information on how he makes decisions while seeking out items, how can we even begin to consider it? Finally, it is crucial to build a legitimate judicial system that operates in the correct area of cybercrime. But in my view, it is best to create a judicial body that is knowledgeable about this subject; they will render the best judgment in this case. Due to the fact that they are highly intelligent in this area.

³⁰ <<http://www.progressbangladesh.com/maximum-14-tears-in-jail-for-cyber-crimes/> [last visited 07th August, 2022].>

3.4. Execution/Remedy

The Bangladeshi government wants to put it into action, but it is completely unprepared right now. However, the government now intends to establish two distinct tribunals in Chittagong and Dhaka.³¹ Government agencies enforce local legislation such the ICT Act of 2006, the Penal Code, and the Digital Security Act of 2012 to protect the cyber sector. The government may also appoint a Deputy Controller and Assistant Controller by official gazette.³² They also have an electronic record reservation room where they can gather and save information.³³ But this is completely insufficient.

The law enforcement agencies in our nation carry out the regulations outlined in those Acts. However, there is no suitable solution, and the agencies won't adequately implicate it since they won't know how to do so for the benefit of society. There are no sections of our laws that expressly state what the implementation system is supposed to be. But sections 56, 57, 67, and 68 of the ICT Act also go into detail about some implementation methods.

In summary, there is no precise strategy for implementation, and the cure won't be adequately explained. Implementation, in my opinion, refers to the act of putting a decision into action or, more specifically, the execution of a plan. What would be done, though? Actually, no suitable action has been taken in this regard, and no effective strategy for countering cybercrime exists. The remedy is therefore always the same. Under the ICT Act of 2006, a cyber victim in Bangladesh has a better chance of receiving the appropriate remedy. The first and only avenue for the legal redress of several cybercrimes in Bangladesh is provided by this statute. It is being attempted through this statute to identify all the potential bases of cybercrime that are currently occurring frequently and that may also occur in the future, such as stealing or harming any text, audio, or video documents, damaging any computer or computer system, hacking, spreading viruses and false information, spreading defamatory information online, changing the source code etc. There are provisions for special Cyber Tribunals (both Original and Appellate), and lighter/severe penalties have been established. The legislation needs to be changed first.³⁴

³¹ <forum.daffodilvarsity.edu-bd/index.php?topic=11293.0>[last visited 7th August, 2022].>

³² Section 18 of The Information Technology Act, 2006.

³³ Section 18(7) of The Information Technology Act, 2006.

³⁴ <http://www.banglajol.info/index.php/NUJL/article/viewFile/18529/12979>[last visited 7th August, 2022].>

I believe that in order to prevent cybercrime, we must first uphold the constitution. 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 for cyberwarfare that may produce a better outcome than any other organizational or legal remedy. Such provisions may be introduced through a constitutional amendment.

The second step is to identify the issues and draft an Act that will allow us to apply this law and provide a framework for finding solutions. Always base a solution on the underlying issue. So, before we can develop a remedy, we must first identify the problem. On the other hand, I believe that we can find a suitable solution to this if the laws are established solely based on cyber and if they are made by scholars. And we need to alter the method of implementation so that we can successfully put this regulation into effect. For example, if we create a system that people are required to uphold or else they won't be able to use the internet.

There is always a danger of such defenses being destroyed because they are not permanent in nature. Nevertheless, technical defense is undoubtedly better than legal remedy in stopping high-tech crimes. Technology-advanced individuals have the ability to breach the security barrier at any time. So, in order to win the war against the aforementioned circumstances, legal and other associated remedies are required. The state may start new initiatives in addition to the current solutions, following in the footsteps of some industrialized, high-tech nations.

We need to create a new branch of police who are well educated on the basis of the internet for a digital Bangladesh. Cyber criminals are not adversaries of any particular country or region; rather, they are the world's common enemies. Citizens of the twenty-first century must band together to fight common enemies. And the adversaries are using the internet as a weapon. To combat all crimes, including cybercrime, the police force must be able to meet technological challenges through global collaboration. The United Kingdom, the United States of America, India, Malaysia, and other developed countries have established special police wings to combat cyber warfare. Bangladesh must create such a body or else she will be attacked repeatedly.

On July 23, 2009, North Korea twisted 'Korea Internet and Security Agency'²⁵, a government agency uniting three of its preceding internet technology organizations. This agency will now work to make North Korea a stronger and more secure advanced country in terms of internet use. Such

organizations have also been established in India and a few other countries. Given the current state of internet use and rising cybercrime in Bangladesh, the government must establish such agencies."³⁵

These organizations, like security-oriented intelligence, rely heavily on the internet. Capturing and receiving malicious software, disassembling, sandboxing, and analyzing viruses and Trojans, monitoring and reporting on malicious attackers, disseminating cyber threat information, and so on are examples. This dog concept is not novel. The 'Shadow Server Foundation,' which was founded in 2004, is an example of a Watch Dog Group. These can be both individual and governmental in nature. There is currently no such organization in Bangladesh, but with the escalating cyber threats, these dog groups could be one of the most important components in developing Bangladesh as a developed country, particularly in internet technology.

Last and most crucial in establishing such things is public awareness. It is crucial to understand the value of the internet, how it is used and misused, and what cybercrime is.

³⁵ <<http://www.banglajol.info/index.php/NUJL/article/viewFile/18529/12979>[last visited 7th August, 2022].> accessed 7 August 2022.

CHAPTER - 4

CHALLENGES FOR IMPLEMENTATION OR COMBATING CYBER CRIME

4.1. National Plan

Making a new law is highly challenging. Because of this, we have to go through a very difficult process if we want to make a new legislation. First and foremost, we must develop a national strategy to address these sorts of crime. The government needs 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 laws, such as:

4.1.1. Recognizing the issue

To start, we must acknowledge the issue, which is really a contemporary issue. Today, everyone is completely plugged into the internet, which leads to crime being committed online by people who are just like regular criminals. Therefore, we must identify the different types of offenses before making a judgment. But I can't discover any sections of our legislation that outline how to comprehend the issue.

4.1.2. Partnerships and shared responsibility; individual crime

Cybercrime is a sort of individual crime, albeit it can occasionally be committed by a collective. While we can't fight it alone, we can implicate it by working in groups or partnerships and taking personal responsibility. We can then minimize it. Our Acts make it clear who has the authority to conduct investigations and how to do so. However, the way they operate in this field has not been mentioned.³⁶

4.1.3. A prevention-centric approach

No sections of our laws can elaborate on the method of focusing on prevention. But in order to stop that crime permanently, we must set a target. This crime will end if we are required by the law to set the aim for preventing it.

³⁶ <<https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx>> accessed 7 August 2022.

4.1.4. Balancing security freedom and privacy

Users' independence, creativity, and innovation are the cornerstones of the internet. We must strike a balance between the rights of internet users and national policy in our efforts to improve online security and combat cybercriminals. We should respect each person's right to privacy. However, we regret to inform you that our Acts do not have any provisions for this kind of initiative policy.

4.2. Law Makers on the Basis of Cyber

A nation must create a new entity that is completely highly intelligent in the sphere of cyberspace or the internet in our contemporary era of digitalization. No such body exists in our nation to create laws based on internet usage. Laws are created by natural intellect. They don't have a very strong online presence. The issue now is how they can pass legislation on something when they don't know much about it. Because they can only see the issues, they are unable to address them. And they create laws that are inappropriate for that circumstance.

4.3. Law Ministry on the Basis of Cyber

Regarding internet-related issues or topics relating to the cyberspace, we do not have any specific ministries. But in our society now, it is a significant issue. Like the natural criminal, many people are committing these crimes quickly. because we don't have a guardian over this. If our government establishes a ministry, we will be protected from online crooks. Considering that this ministry is our protector. And in my opinion, if we have a guardian, we will be able to pass laws based on our needs, and this ministry comprises of academics.

4.4. Public Awareness about Cybercrime

It is crucial to educate the public on all issues related to cybercrime. They may commit such an offense if they do not have a good understanding of the subject. If we look at the situation carefully, we can see that we are currently completely unaware of cybercrime. We are committing these kinds of offenses as a result.

4.5. Internet Based Education

Future generations are today's children. However, the foundation of our educational system is literature. Through their teachings, we must educate children about cyber-related issues. If not, they will be charged with a cyber offense due to their lack of knowledge in this area. The Bangladeshi government needs to take action. Where are they, though? Making laws alone is not

enough to protect society; laws must also be put into practice. Internet-based education is therefore crucial for preventing cybercrime.

4.6. Digital Security

Because of the weak security in our country, numerous thieves have successfully hacked our system on numerous occasions. It won't be done if our security is difficult. We also have the 2016 Digital Security Act. But this Act is similar to the ICT Act of 2006. The Act does not go far enough to stop cybercrime. The toughest security Act should be created. If not, our nation will gradually suffer.

4.7. Investigational Power and Investigational System

Our laws stipulate that only a sub-inspector may look into it. What will happen if he is not knowledgeable about that subject, though? It fully damaged because of his illiteracy regarding internet related subject. This criminal investigative process is comparable to other crimes. Are other crimes and cybercrimes similar? No, never this is not same at all. Therefore, why is the inquiry process the same? I'm not sure. If the investigation involved academics who are knowledgeable about cybercrime. When it happens, we can rely on it and get a superior investigation report. The mechanism for investigations is similar to other situations. However, as it is a wholly IT-based crime, we must adhere to and rely on the IT system in order to receive the necessary information. Perhaps it won't be adhered to in our country.

CHAPTER - 5

CONCLUSION: FINDINGS AND RECOMENDATIONS

5.1. Introduction

By doing this research, I want to advise our government to create a suitable cyber law and a separate, independent authority to conduct exclusive investigations. I want to propose creating a ministry that would also adorn the body as needed. There is a new communication system in use today, and the digital technology system has undergone significant changes. However, the internet's security system is not very robust. This investigation led me to the conclusion that Bangladesh faces a significant cyber threat. Bangladesh is a developing country in terms of technology, and the number of internet users is growing quickly, but no one is in charge of regulating them. Because of this, we can identify issues such as bank robbery and the production of obsessional movies on the internet via a computer or mobile device. The internet is used for many kinds of criminality, but we lack the right institutions to deal with it. We can see that a lot of cybercrimes have attracted public attention in Bangladesh during the past few years. Cybercrime in Bangladesh includes, among other things, the hacking of government-run websites and the publication of private information about well-known and respected citizens of the nation. In essence, it is obvious that we must pass a legislation regarding it. And we need to create a different body to enforce it.

5.2. Criticisms

Our law, where is it? Our legislators are absent. Exists a sector of cybercrime here? No, not at all. We have law, but it does not have a cyber foundation. We also have a sizable number of scholars who serve as law makers, but are they experts in that field? I don't think so, as this is a very recent issue in our nation. Although it might be new, we're looking for a law to address it. Since that is a really dangerous issue. We want an internet data center that is secure. Based on

this, we don't have any specific ministries. We are not well educated on the subject. To learn about cybercrime, we must make it a required subject in our schooling.

5.3. Findings

Based on my research, I discovered some issues in Chapter 2. That: -

- Our Information and Communication Technology Act of 2006 is insufficient to deal with cybercrime.
- Only a few sections of the Information and Communication Technology Act of 2006 deal with cybercrime, but this is unclear.
- Punishment is not appropriate for the crime sought, as stated in the Information and Communication Technology Act of 2006.
- There is no mention of all cybercrime.
- It is the law of all communication systems.
- The government passes the Digital Security Act of 2016, but it is the same as the Information and Communication Technology Act of 2006. There will be no fundamental changes discovered.
- The Digital Security Act of 2016 defines what constitutes lawful and unlawful access. It is not so clear, and it is highly contentious.
- There is no section that discusses how to combat cybercrime.
- The Pornography Act of 2012 and the Child Pornography Act were also enacted to protect children from pornography on the internet.
- This Act will not cover all aspects of cybercrime. Nobody posts porn on the internet; this is the process, but where is the solution?
- Our Penal Code never mentions cybercrime, but section 13 describes similar offenses.
- Bangladesh Telecommunication Act 2001 is deals only cellular network. It is not very modern and does not address cybercrime at all.

5.4. Recommendations

First and foremost, I believe it is critical to create a new understanding of the internet for all. We must be aware of this. Based on this research, I propose the following solutions:

- First and foremost, we must recognize the issue.
- We must pass a law solely on the basis of cybercrime.
- An individual ministry is very important to take care of this law.
- This law must be implemented by a unique and independent body. Who can excess their power as like police or another law enforcing agencies.
- This body must appoint academics with expertise in the information technology sector.
- Establishing a cyber-forensics lab is crucial.
- We desire a virtual storefront.
- If we implement a system that prevents anyone from using the internet without entering their NID number or birth certificate number.
- We must set up an internet-based teaching system.
- The most crucial factor in the implementation of this law is public awareness.

I believe that if we implement this suggestion, the internet will finally become safe.

5.5 Conclusion

In the evening, it is crucial to emphasize that without adequate internet education, we cannot create a secure online environment. Making solid laws based on the circumstances is crucial to creating a digital nation. We might be able to find the solution if we heed that advice. It is crucial to consider all cybercrimes to be civil offenses. We need to instantly defend our nation.

BIBLIOGRAPHY

Books

1. Ahmed D, A Text Book On Cyber Law In Bangladesh (1st edn, National Law Book Company 2012)
2. Ryder D, Guide To Cyber Laws (2nd edn, Wadha & Company 2005).

List of Statutes

1. The Information and Communication Technology Act, 2006
2. Digital Nirapotta Ain 2018
3. The Penal Code, 1860 (Act No. XLV of 1860)2.
4. Bangladesh Telecommunication Act 2001
5. Criminal Code of Procedure 1898
6. Pornography Act 2012
7. The National Information and Communication Technology (ICT) Policy (October, 2002).

Journals

1. Duggal P, 'Causes Of Cyber' (2016) 3 International Journal of Computer Science and Information Security.
2. Biswas R, 'Cybercrimes Need More Attention' <<http://www.cybercrimeslaw.net>> accessed 02 September 2022.

Websites

1. 'BDLD - A Leading Law Magazine/Journal In Bangladesh' (Bangladesh Law Digest (BDLD), 2022) <<http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/>> accessed 2 September 2022
2. 'Bangladeshis Hack 20,000 Indian Websites' (Gadgets 360, 2012) <<http://gadgets.ndtv.com/internet/news/bangladeshis-hack-20000-indian-websites-224516>> accessed 2 September 2022.
3. Ahmed F, 'Bangladesh Muslims Torch Buddhist Shrines, Police Say | CNN' (CNN, 2012) <<http://edition.cnn.com/2012/09/30/world/asia/bangladesh-muslim-buddhist-violence/>> accessed 1 September 2022.
4. 'Hackers Bugged BB System In Jan' (The Daily Star, 2016) <<http://www.thedailystar.net/frontpage/hackers-bugged-bb-system-jan-789511>> accessed 1 September 2022.
5. 'BDLD - A Leading Law Magazine/Journal In Bangladesh' (Bangladesh Law Digest (BDLD), 2016) <<http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/>> accessed 3 September 2022.
6. <<http://sufi-faruq.com/en/combating-cybercrime-a-bangladeshi-perspective-2/>>
7. 'BDLD - A Leading Law Magazine/Journal In Bangladesh' (Bangladesh Law Digest (BDLD), 2015) <<http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/>> accessed 1 September 2022.
8. <<http://www.progressbangladesh.com/maximum-14-tears-in-jail-for-cyber-crimes/>[last visited 07th August, 2022].>
9. <<http://www.banglajol.info/index.php/NUJL/article/viewFile/18529/12979>[last visited 7th August, 2022].> accessed 7 August 2022.
10. <forum.daffodilvarsity.edu-bd/index.php?topic=11293.0[last visited 7th August, 2022].>
11. <<https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx>> accessed 7 August 2022.