CHAPTER 1

INTRODUCTION

1.1. Statement Of The Problem

Late enacted Information and Communication Technology Act, 2006 has defined Digital Evidences Act crime and brought this crime under our criminal jurisprudence. However, there are many other things need to be included in the Act and we have to enact and implement appropriate laws to address the problem of Digital Evidences Act crime.[1] In Bangladesh there are no sufficient laws or other instruments to prevent Digital Evidences Act crime mentioned above. Bangladesh is a developing country. Its technology is also being developed day by day. The problems I sorted out in this regard are as follows- Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes within the ambit of Digital Evidences Act crime.[2] or Any unlawful acts wherein the computer is either a tool or target or both.[3] are called Digital Evidences Act crime. It is the newest member of crime world. Digital Evidences Act crime is very different from the use of computers for a traditional activity. Its multi-million problems by using computer to commit Digital Evidences Act terrorism, financial cheating, by giving attractive advertising in the website or enticement by email, credit card frauds, IPR violation, harassments, fraud, hackers, pornography, virus introduction, stalking, surveillance, theft, disabling computer data, software and hardware, theft of valuable information, international money laundering through internet and online gambling are the most using way to cheating Bangladeshi people.

[1] <http://www.thedailystar.net/law/2009/06/03/watch.htm> Accessed on 02.03.2025

[2] <http://jabalpurpolice.org/cyber_crime.php> Accessed on 02.03.2025

[3] <http://jabalpurpolice.org/cyber_crime.php> Accessed on 02.03.2025

- The problem of Digital Evidences Act crime in Bangladesh is burning question. Now-a-days we observe that different sectors, such as education, bank and multinational company are affected by Digital Evidences Act crime.
- The punishment provided in the case of Digital Evidences Act law is not enough.
- There is no authority to monitor the misuses of Digital Evidences Act law.

So, considering above mentioned in this research I am going to deal with these problems.

1.2. Importance Of The Study

With the advent of Information Technology (IT), Internet and Information and Communication Technology (ICT), the world civilization is facing new dimension of criminal offence. Digital Evidences Act law is a new phenomenon of modern technological development. This is also a new concept in our country. About Digital Evidences Act crime in Bangladesh there is no available books, journals or effective research or work is made on it. For this reason I have chosen to work on "*Digital Evidences Act Crime in Bangladesh*". In my research I will focus on the concept of Digital Evidences Act crime and many other related things so that students, teachers, lawyers, policy makers and overall our country will be benefitted by the findings of my research. Research is an important element of modern system of legal education. It performs several related functions: attaining theoretical knowledge, practical training & a general education contributing to proper legal reasoning, effective communication & ethical responsibility. Research methodology is important for researchers in a number of ways. A student should learn about research so that he can critically analyze information on a variety issues. Legal research is also important for lawyer, who as a real-life problem solver should be familiar with those areas of law in which he claims to have expertise. Research is critically important for initiating reform & change in a society. Research can initiate a new theory of variety

issues, challenge old one or help in clarifying existing theory. The findings of research may be helpful to bring about deserve changes in existing institutions.[4]

1.3. Objectives Of The Research

The main objectives of this research are:

1) To explore the nature of contemporary Digital Evidences Act crimes and its consequences in Information and Communication Technology (ICT).
2) To analyze the related Digital Evidences Act Laws of Bangladesh.
3) To examine the legal measure against the Digital Evidences Act Crimes in Bangladesh.

1.4. Research Methodology

To prepare the research paper some secondary data have been collected and analyzed from the various sources. Such as, most of the information has been furnished through internet, books, journals, article's, various papers as well as others field. Although the research methodology consisted of both a quantitative and qualitative approach, in this research mainly qualitative method have been followed. Moreover to make this research paper effective, I have collected materials from the oral sources and other related sources.

1.5. Sources And Materials

To prepare this research paper some secondary data has been collected and analyzed from the various sources. Such as: Most of the information has been furnished through internet, books, journals, article's, and various papers as well as others field.

1.6. Review Of Literature

A few numbers of writers have written books on the Digital Evidences Act Law in Bangladesh perspective. They have expressed their concept in deferent ways. Some of the books are reviewed below:

[4] Abdullah Al Faruque, *Essentials of Legal Research,* (2nd ed., Dhaka: Palal prokashoni, 2010), pp. 14-15.

(1) Prof. Md. Borhan Uddin. (1st Edition: January, 2008 & February, 2010), Principles of Digital Evidences Act Law, Shams Publications, Dhaka.

This book contains different aspects. The author this book had divided into thirty one chapters. The new enacted laws are included in this book. The subject has been approached in a legal perspective with emphasis on recent development in the field of Digital Evidences Act law and Digital Evidences Act crime. The author has endeavored to achieve the objects of Digital Evidences Act law and Digital Evidences Act crime. To know about Digital Evidences Act crime and its nature this book may help in number of different ways. Enough topics are written down and the author also has mentioned some Digital Evidences Act Crime Cases. But this book is not sufficient to know deeply about the topic and did not mention about the history of digital computer, internet and the genesis object and scope of the IT. There is no any significant suggestion about the future of Information and Communication Technology (ICT) sector of Bangladesh.

(2) Dr. Zulfiquar Ahmed (1st Edition: March, 2009), A Text Book on Digital Evidences Act Law in Bangladesh, National Law Book Company, Dhaka-1205.

This book contains different aspects. The main objective of this book is to serve the mission to spread Digital Evidences Act Law literacy. In this book the writer has been stressed mainly on the Information and Communication Technology Act, 2006. And he mentioned the topic broadly and discussed Digital Evidences Act Law of Bangladesh perspective. The author has discussed many important topics on Chapter Eight such as:

- Its Crime, Investigation, Judgment and Punishment.
- The Establishment of Digital Evidences Act Tribunal, Enquiry, Trial and Appeal of Crimes etc.
- Establishment of Digital Evidences Act Appeal Tribunal etc.

The history and definition of this book it is supposed to be discussed in the first chapter but the writer has mentioned it on chapter Eight.

I think that, this is the new concept in Bangladesh. So, my suggestion is the definition and history of the Information and Communication Technology (ICT) sector of Bangladesh should have mentioned at the first.

> **(3)** Dr. Farooq Ahmad (2nd Edition: 2005), Digital Evidences Act Law in India (Law on Internet), New Era Law Publications, Law Book Publishers, 1159, Outram Lines, Near Kingsway Camp, Delhi 110009.

This book contains different aspects. To know about Digital Evidences Act crime and its classification this book may help in number of different ways. But this book is not enough to know more about the topic and did not mention the definition of the Digital Evidences Act Law, Digital Evidences Act Crime and its concept. It would be clearer if the definition of the Digital Evidences Act Law, Digital Evidences Act Crime and its concept broadly discussed. There is no any significant suggestion about the future of Information and Communication Technology (ICT) sector of today's and future world.

> **(4)** Justice Yatindra Sign (2nd Edition: 2005), Digital Evidences Act Laws, Universal Law Publishing co. Pvt. Ltd. C-FF-1A, Ansal's Dilkhush Industrial Estate, G.T. Karnal Road, Delhi- 110033.

This book contains different aspects. The author has included cases decided since then, chapter 1 of the book which deal with the IT act has been arranged so as to broadly refer to the chapters and sections of the IT act.

This book is not sufficient to know deeply about the topic and it has not mentioned the history of digital computer, internet and the genesis object and scope of the IT. This book has not mentioned the definition of the Digital Evidences Act Law, Digital Evidences Act Crime and its concept and the entire topic are very short form. There is no any significant suggestion about the future of Information and Communication Technology (ICT) sector.

CHAPTER 2

Historical Background

2.1. Introduction

We are living in a digital world where computers are not just an ordinary thing anymore but a "necessity" to our everyday life. The internet in Bangladesh is growing rapidly. It has given rise to new opportunities in every field we can think of – be it entertainment, business, sports or education. With the advent of Information Technology (IT), Internet and Information and Communication Technology (ICT), the world civilization is facing new dimension of criminal offence. This chapter firstly identifies the definition and then focuses on history and background of Digital Evidences Act crime, nature of Digital Evidences Act crime, Classification of Digital Evidences Act Crime. Finally the chapter analyses the Challenge of Digital Evidences Act Crimes, Characteristics, and victims of Digital Evidences Act Crime.

2.2. Definition Of Digital Evidences Act Crime

Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes within the ambit of Digital Evidences Act crime.[5] or Any unlawful acts wherein the computer is either a tool or target or both.[6] are called Digital Evidences Act crime.

The term *'Digital Evidences Act crime'* has been evolved from two words *'Digital Evidences Act'* and *'crime'*. 'Crime' is more or less known to each individual on his own stand point, while 'Digital Evidences Act' is almost vague in meaning to the same. So if any time anybody uses the prefix 'Digital Evidences Act', we simply mean, he is talking about something is doing online or there has certain networking

[5] < http://jabalpurpolice.org/cyber_crime.php> Accessed on 02.03.2025
[6] < http://jabalpurpolice.org/cyber_crime.php> Accessed on 02.03.2025

system. Actually anything related to Internet falls under the Digital Evidences Act category.[7]

Computer crime or Digital Evidences Act crime is a form of crime where the Internet or computers are used as a medium to commit crime. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement Child pornography, and child grooming.[8]

Digital Evidences Act crime 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. Digital Evidences Act crime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.[9]

2.3. History And Background Of Digital Evidences Act Crime

The internet has revolutionized how individuals interact with each other. After four years of the Internet, fifty million people are connected to this global network. It took the radio thirty-eight years to reach fifty million users, and a mere sixteen years for the computer to reach fifty million users. The popularity of the Internet is growing exponentially.[10] The first recorded Digital Evidences Act crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. This is the first recorded Digital Evidences Act crime.[11] Interpol was the first international organization dealing with computer crime and penal legislation. In conjunction with an Interpol Conference in 1981, a survey of Interpol member countries on computer crime and penal legislation identified several problems in the application of existing penal legislation. The OECD in Paris appointed in 1983 an expert committee to discuss computer-related crime and the need for changes in the penal Codes. This committee made a proposal that could constitute as a common

[7] M. Abul Hasanat, *'Cyber Crime: An Ill-going Techno - Culture'*, Journal of Law, Vol. 1, no.1 (June 2003), p.15.
[8] <http://en.wikipedia.org/wiki/Cyber_crime> Accessed on: 21.03.2025
[9] < http://www.techterms.com/definition/cybercrime> Accessed on: 21.03.2025
[10]<http://www.associatedcontent.com/article/44605/cybercrime_a_revolution_in_terrorism.html?cat=37> Accessed on: 21.03.2025
[11] R. K. Chaubey, *An Introduction to Cyber Crime and Cyber Laws,* (1st ed., Kolkata: Kamal Law House, 2009), p.137.

denominator between the different approaches taken by the member countries. The Council of Europe appointed in 1985 another expert committees in order to discuss the legal issues of computer-related crime. A summary of the guidelines for national legislatures with liability for international acts only, was presented in the Recommendation of 1989. The UN adopted a resolution on computer crime legislation at 8th U.N. Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba, in 1990. The United Nations Manual on the Prevention and Control of Computer-related Crime was published in 1994. The last part of this historic presentation is the Wurzburg conferences organized by the University of Wurzburg in 1992. These conferences led to 29 national reports, and recommendations for the development of computer crime legislations. Most countries in Europe adopted new penal laws according to the recommendation in the 1980s and 90s. Similar development occurred in the U.S.A. Canada and Mexico also in Asia, where Japan, Singapore, Korea and Malaysia were the leading countries. In Australia, the Commonwealth added computer crime laws to *the Crimes Act* in 1989. Today computers have come a long way, with neutral networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second.[12]

2.4. Nature Of Digital Evidences Act Crime

A Digital Evidences Act criminal can destroy websites and portals by hacking and planting viruses, carry out online frauds by transferring funds from one corner of the globe to another, gain access to highly confidential and sensitive information, cause harassment by e-mail threats or obscene material, play tax frauds, indulge in Digital Evidences Act pornography involving children and commit innumerable other crimes on the Internet. It is said that none is secure in the Digital Evidences Act world. The security is only for the present moment when we are actually secure. With the growing use of the Internet, Digital Evidences Act crime would affect us all, either directly or indirectly.[13]

[12] Ibid, pp.139-140.
[13] Ibid, p.141.

2.5. Tools And Methods Of Digital Evidences Act Crime

Digital Evidences Actcriminals are using numerous illegal tools: *keylogging*—using software or devices to secretly monitor and record keystrokes, enabling espionage activities or the harvesting of personal data; *distributed denial of service* (DDoS)—inundating computer system resources with tasks sufficient to render them unavailable to authorized users; *pharming*—directing traffic from a legitimate Web site to a site controlled by a criminal hacker; *phishing*—illegally accessing an individual's financial data to capture online banking and financial information; and, most recently, *botnets*—networks of infected machines, usually managed by a single command center, that are capable of causing serious damage to networked systems and enabling large-scale identity theft. Hackers obtain botnets commercially, using them to access bank accounts.[14]

[14] <www.ncjrs.gov/pdffiles1/nij/231832.pdf> Accessed on: 05.04.2025

CHAPTER 3

Kinds Of Digital Evidences Act Crime

3.1. Introduction

In Bangladesh most of us only knew a little about computer security threats, the most common were "*virus*" and "*worm*". Let me examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Here is the list of the prevalent Digital Evidences Act Crimes, some of which are more widely spread and harmful. There are two sides of a coin. Internet also has its own disadvantages. One of the major disadvantages is Digital Evidences Act crime – illegal activity committed on the internet. The internet, along with its advantages, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like hacking, virus, trojans and worms, Digital Evidences Act pornography, Digital Evidences Act stalking, Digital Evidences Act terrorism, Digital Evidences Act crime related to finance, Digital Evidences Act crime with mobile and wireless technology, phishing, denial of service attack (Dos Attack), e-mail bombing and so on, which invade our privacy and offend our senses.

3.2. Hacking

'Hacking' means unauthorized access to a computer system. It is the most common type of Digital Evidences Act crime 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 information residing in a computer resource or diminishes its value or utility or affects in injuriously by any means; harm any computer, server, computer network or any other electronic system by accessing it unlawfully and in which that person has no legal authority; he commits the offence of "hacking".[15] Whoever commits hacking shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to taka one crore or with both.[16]

The person who commits an offence of hacking is called hacker. Hacker is a person who intends to gain unauthorized access to a computer system. Jargon Dictionary traces the origin of the term 'hacker' to someone who makes furniture with an axe and the term has been used for the first time in 1960's as a badge by hacker culture surrounding the Tech Model Railroad Club (TMRC) at Massachusetts Institute Technology when its members began to work with computers.[17]

Webster's Dictionary defines the term 'hacker' as a computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance.[18]

The word 'hacker' represents now any person-

(a) Who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
(b) Who programmes enthusiastically.

---

[15] Zulfiquar Ahmed, *A Text Book on Cyber Law in Bangladesh,* (1st ed., Dhaka: National Law Book Company, 2009), pp.63 – 64.
[16] The Information and Communication Technology Act, 2006, s. 56(2).
[17] Farooq Ahmad, Ibid, p. 329
[18] Ibid, p. 329

(c) Who enjoys programming rather than just theorizing about programming.

(d) Capable of appreciating hack value, which is defined as the reason or motivation for expending effort toward a seemingly useless goal, the point being that the accomplished goal is a particular programme or one who frequently does work using it or on it.[19]

Examples of Hackings in Bangladesh:

Some Examples of Hacking in Bangladesh are given below:

Recently Indian hacker groups will be destroyed by Digital Evidences Act space as it was announced. Government of Bangladesh has already made an attack by the Indian hacker group – large or small 50 websites. 300 to 400, as well as private organizations and websites have already been attacked. On the other hand, there are hundreds of Indian websites hacked by Bangladeshi hackers. The websites of the government and commercial organizations. Bangladesh started on Thursday. And not only have this but also frequently we are facing liked this problem from last few years.[20]

3.3. Virus, Trojans And Worms

A computer virus is a programme designed to replicate and spread, generally with the victim being oblivious to its existence. Computer viruses spread by attaching themselves to programmes like word processor or spreadsheets or they attach themselves to the boot sector of a disk. A computer worm is a self-contained

[19] Ibid, p. 329

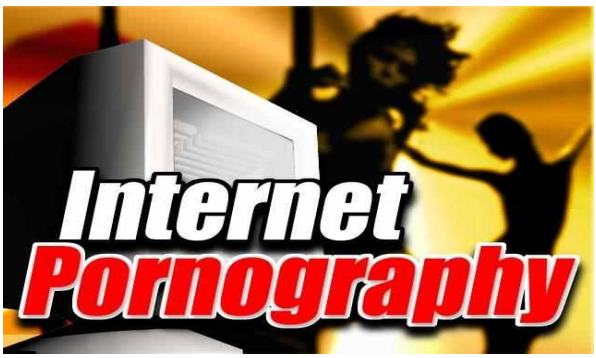
[20] < http://www.dailykalerkantho.com/?view=details&archiev=yes&arch_date=13-02-2025&type=gold&data=Loan&pub_no=791&cat_id=1&menu_id=13&news_type_id=1&index=5> Accessed on: 13.02.2025

program that is able to spread functional copies of itself or its segments to other computer systems. Unlike viruses, worms do not need to attach themselves to a host program.[21] A computer virus is a small software program that spreads from one computer to another computer and that interferes with computer operation. A computer virus may corrupt or delete data on a computer, use an e-mail program to spread the virus to other computers, or even delete everything on the hard disk. Computer viruses are most easily spread by attachments in e-mail messages or by instant messaging messages. Therefore, you must never open an e-mail attachment unless you know who sent the message or unless you are expecting the e-mail attachment. Computer viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Computer viruses also spread by using downloads on the Internet. Computer viruses can be hidden in pirated software or in other files or programs that you may download.[22]

A computer virus is a computer program that can replicate itself and spread from one computer to another. The term "virus" is also commonly, but erroneously used, to refer to other types of malware, including but not limited to adware and spyware programs that do not have a reproductive ability. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by other computers. Malware includes computer viruses, computer worms, Trojan horses, most rootkits, spyware, dishonest adware and other malicious or unwanted software, including true viruses. Viruses are sometimes confused with worms and Trojan horses, which are technically different. A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan horse is a program that appears harmless but hides malicious functions. Worms and Trojan horses, like viruses, may harm a computer system's data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious or simply do

[21] R. K. Chaubey, Ibid, p.143.
[22] <http://support.microsoft.com/kb/129972> Accessed on: 12.04.2025

3.4. Digital Evidences Act Pornography



The growth of technology has flip side to it causing multiple problems in everyday life. Internet has provided a medium for the facilitation of crimes like pornography. Digital Evidences Act porn as it is popularly called is widespread. Almost 50% of the web sites exhibit pornographic material on the Internet today. Pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-ROMs... Furthermore, there are more serious offences which have universal disapproval like child pornography and far easier for offenders to hide and propagate through the medium of the Internet.[23]

3.5. Digital Evidences Act Stalking

Although there is no universally accepted definition of Digital Evidences Act stalking, the term is used in this report to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.[24] Digital Evidences Act Stalking can be defined as the repeated acts harassment or threatening behavior of the Digital Evidences Act criminal towards the victim by using internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, vandalizing victim's property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same

[23] R. K. Chaubey, Ibid, p.144.
[24] <http://www.cyberguards.com/CyberStalking.html> Accessed on: 12.04.2025

has to be treated and viewed seriously. These problems occur on the Internet as well, in what has become known as Digital Evidences Act stalking or on line harassment.[25]

Definition of Digital Evidences Act Stalking:

Stalking is a continuous process, consisting of a series of actions, each of which may be entirely legal in itself. Technology ethics professor Lambèr Royakkers writes that:

"Stalking is a form of mental assault, in which the perpetrator repeatedly, unwantedly, and disruptively breaks into the life-world of the victim, with whom he has no relationship (or no longer has), with motives that are directly or indirectly traceable to the affective sphere. Moreover, the separated acts that make up the intrusion cannot by themselves cause the mental abuse, but do taken together (cumulative effect)."

Digital Evidences ActAngels has written about how to identify Digital Evidences Act stalking:

When identifying Digital Evidences Act stalking "in the field," and particularly when considering whether to report it to any kind of legal authority, the following features or combination of features can be considered to characterize a true stalking situation: malice, premeditation, repetition, distress, obsession, vendetta, no legitimate purpose, personally directed, disregarded warnings to stop, harassment, and threats.[26]

Types of Digital Evidences Act Stalking:

Of women

Harassment and stalking of women online is common, and can include rape threats and other threats of violence, as well as the posting of women's personal information. It is blamed for limiting victims' activities online or driving them offline

[25] R. K. Chaubey, Ibid, p.144.
[26] <http://en.wikipedia.org/wiki/Cyberstalking> Accessed on: 12.04.2025

entirely, thereby impeding their participation in online life and undermining their autonomy, dignity, identity and opportunities.

Of intimate partners

Digital Evidences Act stalking of intimate partners is the online harassment of a current or former romantic partner. It is a form of domestic violence, and experts say its purpose is to control the victim in order to encourage social isolation and create dependency. Harassers may send repeated insulting or threatening e-mails to their victims, monitor or disrupt their victims' e-mail use, and use the victim's account to send e-mails to others posing as the victim or to purchase goods or services the victim doesn't want. They may also use the internet to research and compile personal information about the victim, to use in order to harass her.

By anonymous online mobs

Web 2.0 technologies have enabled online groups of anonymous people to self-organize to target individuals with online defamation, threats of violence and technology-based attacks. These include publishing lies and doctored photographs, threats of rape and other violence, posting sensitive personal information about victims, e-mailing damaging statements about victims to their employers, and manipulating search engines to make damaging material about the victim more prominent. Victims are often women and minorities. They frequently respond by adopting pseudonyms or going offline entirely.[10] A notable example of online mob harassment was the experience of American software developer and blogger Kathy Sierra. In 2007, a group of anonymous individuals attacked Sierra, threatening her with rape and strangulation, publishing her home address and Social Security number, and posting doctored photographs of her. Frightened, Sierra cancelled her speaking engagements and shut down her blog, writing “I will never feel the same. I will never be the same.”

Experts attribute the destructive nature of anonymous online mobs to group dynamics, saying that groups with homogeneous views tend to become more

extreme as members reinforce each other's beliefs, they fail to see themselves as individuals, so they lose a sense of personal responsibility for their destructive acts, they dehumanize their victims, which makes them more willing to behave destructively, and they become more aggressive when they believe they are supported by authority figures. Internet service providers and website owners are sometimes blamed for not speaking out against this type of harassment.

Corporate Digital Evidences Act stalking

Corporate Digital Evidences Act stalking is when a company harasses an individual online, or an individual or group of individuals harasses an organization. Motives for corporate Digital Evidences Act stalking are ideological, or include a desire for financial gain or revenge.[27]

3.6. Digital Evidences Act Terrorism

Digital Evidences Act terrorism may be defined to be "the premeditated use of disruptive activities, or the threat thereof, in Digital Evidences Act space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." The role of computer with respect to terrorism is that of modern thief who can steal more with a computer than with a gun.. No doubt, the great fears are combined in terrorism; the fear of random, violent, victimization segues well with the distrust and out-rights fear of computer technology.[28]

3.7. Digital Evidences Act Crime Related To Finance

There are various types of Digital Evidences Act Crimes which are directly related to financial or monetary gains by illegal means, to achieve this end, the persons in the Digital Evidences Act world who could be suitably called as fraudsters uses different techniques and schemes to be fooled other peoples on the internet. Online fraud and cheating is one of the most lucrative businesses that are growing today in the Digital

[27] <http://en.wikipedia.org/wiki/Cyberstalking> Accessed on: 12.04.2025
[28] Ibid, p.145.

CHAPTER 4

Digital Evidences Under the Evidence Act, 1972

4.1. INTRODUCTION

In today's world information communication system and network security has become a right issues for the reason that rights to information has become more and more important to everyone as information protects and develops human life everyday. Internet has grown in our country, the need has been felt to enact the appropriate Digital Evidences Act laws, which are indispensable to legalize and regulate internet in Bangladesh.

4.2. Need For Digital Evidences Act Law In Bangladesh

Computer has become integral parts of the modern day homes and workplaces. Countries around the world continue to exhibit an encouraging trend of computer usage. Most academic institution has invested in the best technology to keep their students equipped and informed. As for the workplace, there is a gradual trend towards a possible future brimming with 'paperless and selfless offices'. The dependence on computer is increasing by the day as we are faced with better and faster machines geared up to fulfill operations that were not even imagined a few years back.[29] For the past several years, many countries have been concentrating on the awareness on questions of about the governance of Digital Evidences Actspace. The question of who controls the Internet is directly related to the question who wants to control the Internet. From the moment that the Internet was opened up to commercial activity many different groups wanted to dominate, such as user, communication companies, ISPs, and the government. Of them all, the most objected was the government intervention, yet it is governments that have managed to exert the most control. However as Internet has grown in our country, the need has been felt to enact the appropriate Digital Evidences Act laws, which are indispensable to legalize and regulate Internet in Bangladesh. The need for Digital Evidences Act laws was propelled by numerous factors. The arrival of Internet signaled the

[29] Zulfiquar Ahmed, Ibid, pp.49 – 52.

commencement of the rise of new and intricate legal issues. Despite the brilliant acumen of our master draftsman, the requirement of Digital Evidences Actspace could hardly ever be anticipated. As such, the coming of the internet led to the emergence of numerous ticklish legal issues and problem which necessitated the enactment of Digital Evidences Act laws. The existing laws of Bangladesh, even with the most generous and moderate interpretation, could not be interpreted in the light of the promising Digital Evidences Actspace, to consist of all aspect relating to different activities in Digital Evidences Actspace. There are no existing laws that assigned any legal validity or sanction to the activities in Digital Evidences Actspace, as such, before passing Digital Evidences Act Law, email was not "legal" in our country and courts and judiciary in our country had been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the parliament. The Government of Bangladesh responded by coming up with the first Digital Evidences Act law of Bangladesh Digital Evidences Under the Evidence Act, 1972.

4.3 Historical Background Of The Information And Communication Technology Act (Ict) Or Digital Evidences Act Law

Bangladesh Government has recently enacted *Digital Evidences Under the Evidence Act, 1972* The law has been made in the shape of *the United Nations Commission on International Trade Law (UNCITRAL) of 1996*, which is called *UNCITRAL Model Law* on economic commerce. The *Model Law* does not have any force but merely serves as a model to countries for the evaluation and modernization of certain aspects of their laws and practices in the field of communication involving the use of computerized or other modern techniques, and for the establishment of relevant legislation where none exists. The law is sometimes called Digital Evidences Act law and sometimes the law of "Internet" or "Computer". Bangladesh is the 32nd nations in the world that has Digital Evidences Act legislation apart from countries like India, Singapore, France, Malaysia and Japan.[30]

[30] Ibid, p.52.

4.4. Sides Of Digital Evidences Act Law Or Ict Act Of Bangladesh

Digital Evidences Act laws are meant to set the definite pattern, some rules and guidelines that defined certain business activities going through internet legal and certain illegal and hence punishable. *The ICT Act 2006*, the Digital Evidences Act law of Bangladesh, gives the legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic record. One cannot regard government as complete failure shielding numerous e-commerce activities on the firm basis of which this industry has got to its skies, but then the law cannot be regarded as free ambiguities.[31] *The Information and Communication Technology Act (ICT), 2006* also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same have legal validity and enforceability. Some highlights of the Act have been given below:

Chapter I of *the ICT Act 2006* specifically defines some term which are used in ICT sector and Digital Evidences Act legislation for clearing the concept. This chapter also stipulates the jurisdiction and superiority of the Act. Extra regional effect of the Act has been discussed in the chapter.

Chapter II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber. The said chapter also details the legal recognition of Digital Signature and electronic records. Chapter II of *the ICT Act* details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed from, then, notwithstanding anything contained in such law, such requires shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic from;

[31] Ibid, p.53.

and accessible so as to be usable for a subsequent reference.

Chapter III of *the ICT Act* details for application to the attribution, acknowledgement and dispatch of electronic records among parties.
Chapter IV of *the ICT Act* provides rules for secure electronic records & secure digital signature.

Chapter V of the said Act gives a scheme for regulation of Certifying Authorities. The Act envisage a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

Chapter VI of this Act details about applying the security procedure, acceptance of Digital Signature Certificate, obtaining Digital Signature Certificate and Control of Private Key. The duties of subscribers are enriched in this said Act. Chapter VII & VIII of *the ICT Act* talks about penalties, adjudication, investigation, judgment and punishment for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Tk. 1,00,00,000 to affected persons. The Act talks of appointment of any officer not below the rank of a Director to the Government of Bangladesh or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provision of the said Act or rules framed there under. The said Adjudicating Officer has been given the power of a civil court.

Chapter VIII of the Act also talks of the establishing of the Digital Evidences Act Regulations Appellate Tribunal, which shall be an appellate body where appeals against the order passed by the Adjudicating Officer, shall be preferred.

Chapter – VIII of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of police.

Chapter IX of the Act details about police servant, protection of action taken in good faith. The said Act also proposes to amend *the Penal Code, 1860, the Evidence Act, 1872, the Bankers' Books Evidence Act, 1891* to make them in tune with the provision of *the ICT ACT.*[32]

4.5. Objective Of The Ict ACT, 2006

The preamble of *the ICT Act, 2006* declares that, an Act to provide legal recognition for transaction carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternative to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend *the Penal Code, 1860, the Evidence Act, 1872 and the Bankers' Books Evidence Act, 1891* and for matters connected therewith or incidental thereto.

The object of *the ICT Act, 2006*, has been illustrated by the Law Commission's Final Report to give effect to the following purposes:

i. to facilitated electronic communications by means of reliable electronic records;

ii. to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

[32] Ibid, pp.53-55.

iii. to facilitate electronic filing of documents with government agencies and statutory corporation, and to promote efficient delivery of government services by means of reliable electronic records;

iv. to minimize the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transaction;

v. to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and

vi. to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to faster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.[33]

4.6. Establishment & Jurisdiction Of Digital Evidences Act Tribunal In Bangladesh

Government of Bangladesh by gazette notification, for the purpose of quick and effective trial of crimes committed under the Act, may establish one or more Digital Evidences Act tribunal, sometimes which is stated later as tribunal under *section 68(1) of the ICT Act*. The Digital Evidences Act tribunal that is stated in section (1) of the section will comprise of a session judge or an assistant session judge appointed by the government with consulting with the Supreme Court; and such a judge appointed will be introduced "judge, Digital Evidences Act tribunal".[34]

[33] Ibid, p.57.
[34] The Information and Communication Technology Act, 2006, s. 68(2).

4.7. Establishment & Jurisdiction Of Digital Evidences Act Appellate Tribunal In Bangladesh

The ICT Act envisages the establishment of the Digital Evidences Act Appellate Tribunal at one or more places as the government may deem fit. *Section 82(1) of the ICT Act* provides that the government shall, by notification in the Official Gazette, establish one or more appellate tribunals to be known as the Digital Evidences Act Appellate Tribunal.[35] The Digital Evidences Act Appellate Tribunal shall have the power to hear and settle the appeal made against the judgment of Digital Evidences Act tribunal and session court.[36] The appeal tribunal will have authority of supporting, canceling, changing, or editing the judgment of the Digital Evidences Act tribunal.[37] The decision of the appellate tribunal will be final. The Digital Evidences Act Appellate Tribunal does not seem to be vested with any original jurisdiction; it has been vested with the powers of a Civil Court in respect of, interalia,

i. Summoning and examining of witnesses
ii. Requiring production of document
iii. Receiving evidence
iv. Issuing commissions and
v. Reviewing its decisions.[38]

4.8. Digital Evidences Act Law And Its Weakness

The world over Digital Evidences Act crime has taken deep root and the use of Digital Evidences Actspace by sophisticated Digital Evidences Act criminals has assumed serious proportion today. Criminals and terrorists associated with drug trafficking, terrorist outfits are employing Internet for anti social; anti national and criminal activities with impunity. Terrorist groups are deftly using Internet for

[35] Ibid, s. 82(4).
[36] Ibid, s. 83(1).
[37] Ibid, s. 83(2).
[38] Zulfiquar Ahmed, Ibid, pp.150-52.

passing on information with regard to executing various terrorist acts having serious negative impact on human life. The Digital Evidences Act-terrorists have even acquired the capability to enter computer systems using "logic bombs" (coded devices that can be remotely detonated), electromagnetic pulses and high-emission radio frequency guns, which blow a devastating electronic wind through a computer system. The hackers have gone to the extent of distributing free hacking software— Rootkit, for instance— to enable an intruder to get root access to a network and then control as though they were the system's administrators. Many instances of Digital Evidences Act crime involve techno-trespass and unauthorized access to the computer system and data or programmes stored in computers. This access could be without authorization or exceeding the authorization given to an individual. The un authorized access may lead to theft, alteration or destruction of data, tampering with computer programmes or other software, damage to computers or computer systems including damage to data stored on storage devices, such as hard disks, floppy disks, CD-ROMs, etc. This would, in turn, lead to serious financial loss to the organisation. Thus computer crime today has emerged as a challenge for criminal justice system and law enforcement. Studies have shown that computer criminals are generally computer professionals or computer-literate persons and are not history sheeters and mostly without previous criminal record. Studies also show that the threat is mostly from employees or from those with access to the system, such as maintenance personnel, hardware and software vendors, etc. however, external threats via remote access have shown an increasing trend.

4.9. Criticisms Of The Ict Act, 2006

The ICT Act has identified some critical situation, which is not clear to our archaic legal provisions. The law does something regulate the social norm and then control of information technology. Ever since the passing of *the Information and Communication Technology Act* by parliament, a lot has been said both for and against the Act. Although the newly enacted Digital Evidences Act Law has some weakness, something is better than nothing. The criticism of the Digital Evidences Act Law of Bangladesh is given below:

Internet is a borderless medium; it spread to every corner of the world where life is possible and hence is the Digital Evidences Act criminal. Then how come is it possible to feel relaxed and secure once law is enforced in the nation?

The Act initially was supposed to apply to crimes committed all over the world, but nobody knows how can this be achieved in practice, how to enforce it all over the world at the same time?

Recently Indian hacker groups will be destroyed by Digital Evidences Act space as it was announced. Government of Bangladesh has already made an attack by the Indian hacker group – large or small 50 websites. 300 to 400, as well as private organizations and websites have already been attacked. On the other hand, there are hundreds of Indian websites hacked by Bangladeshi hackers. The websites of the government and commercial organizations. Bangladesh started on Thursday.[39] And not only have this but also frequently we are facing liked this problem from last few years when our country is being developed. So, now after considering this can we say we are rightly protected?

Draconian Powers to Police Officers: The draconian powers have been given to police officers that a police officer not below the rank of an Inspector of Police (IP), or any other officer of the Government authorized by the Government in this behalf for purpose of investigating and preventing the commission of a Digital Evidences Act

[39] <http://www.dailykalerkantho.com/?view=details&archiev=yes&arch_date=13-02-2025&type=gold&data=Loan&pub_no=791&cat_id=1&menu_id=13&news_type_id=1&index=5> Accessed on: 13.02.2025

crime under section 80 of the ICT Act-2006.[40] The unrestricted power given by *the ICT Act* to the said IP includes the power 'to enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or being about to commit any offences under this Act'.[41] It is very much possible that the given power may be misused and abused by the said police officers. This law has given more power to police officer in case of arresting Digital Evidences Act criminals, albeit Digital Evidences Act crime detection is very difficult. So, this is similar to *section 54 of the Criminal Procedure Code* in case of harassment to public.

Implementation of Global Digital Evidences Act Law: Implementation of the law is a big question mark for any nations' law enforcing agency. The implementation of the global Digital Evidences Act law is a big challenge without any law enforcing agencies. But countries can take the lead in implementation the law within their national boundaries. Like the US, this has Digital Evidences Act squatting laws that make Digital Evidences Act squatting is a punishable offence. But other countries are very confused and Bangladesh is one of those countries. In fact, *the ICT Act 2006* has a provision wherein the law is not only applicable to Bangladeshi's netizens but also to any contravention or any violation done by anybody anywhere in the world is also liable to the penalties under section 84, which is very impractical unless Digital Evidences Act law related global agreement is in existence. The provision in section 84 is not clearly defined as to how and what particular manner, this *ICT Act* shall apply to any offence or contravention there-under committed outside of Bangladesh by any person. *The ICT Act* does not provide extra-territorial jurisdiction or multi-territorial jurisdiction to law enforcement agencies, but such powers are basically ineffective. This is because Bangladesh does not have reciprocity like EU countries and extradition treaties with a large number of countries. "Domain Name" is the major issue, which related to Internet thoroughly. But the ICT Act, 2006 does not define "domain Name" and the rights and liabilities. "Domain Name" owners do not find any mention in *the ICT Act*. There is no provision about the Intellectual

[40] The Information and Communication Technology Act, 2006, s. 80.
[41] The Information and Communication Technology Act, 2006, s. 79.

Property Rights of "domain Name" owners. These need proper attention. *Section 56 of the ICT Act, 2006*, that the order of the Government appointing any person as the Presiding officer of a Digital Evidences Act Appellate Tribunal shall be final and shall not be called in question in any manner and no Act or proceeding before a Digital Evidences Act Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Digital Evidences Act Appellate Tribunal. The said provisions is a violation of the Fundamental rights of the citizens as are enshrined in *Chapter III of the Constitution of Bangladesh* and the said provision is not convenient and is likely to be struck down by the courts. The Government cannot claim immunity in appointment to Digital Evidences Act Appellate Tribunal, as the same is contrary to the spirit *of the Constitution of Bangladesh*. So, under *the Constitution of Bangladesh*, all proceeding and Act of the Digital Evidences Act Appellate Tribunal are null and void-ab-initio.[42]

Understanding the essential need of security all developed countries have taken steps to address the problem. On the other hand developing countries are far away from being able to guarantee these rights. Threats to the information technology were emerging on the content level as well as on the network level and on the physical level. Information security could however not be achieved by technology alone. In order to respond to network threats and create a secure information technology, both comprehensive prevention measures and enforcement measures are necessary.

[42] Zulfiquar Ahmed, Ibid, pp.66-69.

CHAPTER 5

General Conclusion

5.1. Introduction

The subject of Digital Evidences Act crime is high on the international concern today, not only because of its numerous significance, but also because of its impact on international peace, security and stability. In Bangladesh, Digital Evidences Act crime has to be voluntary and willful, an act or omission that adversely affects a person property. This chapter deals with a summary of findings of this research and recommendation. It firstly discusses the summary of findings of this research. Secondly, this chapter deals about the recommendation of mine which I found from this research.

5.2. Recommendation

The following recommendations can be taken under consideration for the betterment of the present conditions.

- The existing law is not sufficient to provide compensation to victims of the Digital Evidences Act crime for injuries caused or loss suffered by them due to the offender's Digital Evidences Act act.
- The government may constitute a separate authority to monitor the abuse of Digital Evidences Act.
- Digital Evidences Act crime related cases could be adjudicated under the Druto Bichar Tribunal.
- Regular training campaigning should be arranged for the skill development of experts.

This study confirms that Bangladeshi peoples using the internet are in risk it is found by this research that most of the people of Bangladesh are not more conscious to use the internet rightly. So, people have to more conscious about the using of internet in the proper way. The main reason behind this situation is lack of proper education about using internet and as such this system is also liable to misuse the internet technology. So, our Government has to take adequate movement to ensure

the proper education to the mass people for using the internet and information technology in an appropriate way. On the other hand, now-a-days, most of young generation using Digital Evidences Act and a large number of them faced with Digital Evidences Act criminals. But in our country, there is no monitoring body or system to control the various use of Information Technology. It is a matter of great sorrow that, in our laws this issue is almost vague. So, we need an amendment on Information and Technology Communication Act-2006.

5.3. Conclusion

As we move forward into the 21st century, technological innovations have added the way for us to experience new and wonderful conveniences in the how we are educated, the way we shop, how were entertained and the manner in which we do business. It is not possible to eliminate Digital Evidences Act crime form the Digital Evidences Act space. But it is possible to check them or under control. If we look to the history then we can see that no legislation has succeeded in totally eliminating crime from the world. The only possible step is to make people aware of their rights and duties and further making the application of the laws more stringent to check crime. Undoubtedly the ICT Act is a historical step in the Digital Evidences Act world. Besides this it cannot be denied that there is a need to bring changes in the IT Act to make it more effective. The Penal Code, 1860 is not sufficient to protect the needs of new crimes emerging from internet or computer. Though there are some laws and convention, they cannot be implemented due to some technical difficulties like procedural complexities and lack of proper executing system. Taking these advantages, the criminals are occurring serious crimes like Hacking, Sending malicious mails, spreading vulgar pictures, Digital Evidences Act terrorism and illegal using of intellectual properties. It causes harm to the privacy of individuals as well as creates threat to the international peace and harmony. Now it is the demand of time to prevent such type of crimes for keeping individual privacy as well as international peace and security. Every country of the world should enact effective legal provisions within their national boundaries to protect Digital Evidences Act crimes.

REFERENCES

BOOKS

- Abdullah Al Faruque, *Essentials of Legal Research,* (2nd ed., Dhaka: Palal prokashoni, 2010).
- Farooq Ahmad, *Digital Evidences Act Law in India (Law on Internet),* (2nd ed., Delhi: New Era Law Publications, 2005).
- R. K. Chaubey, *An Introduction to Digital Evidences Act Crime and Digital Evidences Act Laws*, (1sted., Kolkata: Kamal Law House, 2009).
- Zulfiquar Ahmed, *A Text Book on Digital Evidences Act Law in Bangladesh*, (1st ed., Dhaka: National Law Book Company, 2009).
- Md. Borhan Uddin, *Principles of Digital Evidences Act Law,* (1st ed., Shams Publications, Dhaka, 2010).
- Yatindra Sign, *Digital Evidences Act Laws,* (2nd ed., Universal Law Publishing co. Pvt. Ltd. 2005).

STATUTES

- The Information and Communication Technology Act (ICT), 2006.

JOURNAL

- M. Abul Hasanat, 'Digital Evidences Act Crime: An Ill-going Techno - Culture', *Journal of Law*, Vol. i, no.1 (June 2003).

NEWSPAPER

- The Daily Star
- The Daily Prothom Alo
- The Daily Kalerkontho

INTERNET

- http://www.associatedcontent.com/article/44605/Digital Evidences Actcrime_a_revolution_in_terrorism.html?cat=37
- www.ncjrs.gov/pdffiles1/nij/231832.pdf
- http://www.pcworld.com/article/205309/65_of_web_users_are_victims_of_ Digital Evidences Actcrime.html
- http://spectrum.ieee.org/riskfactor/telecom/security/over-1-million-Digital Evidences Act-crime-victims-a-day-in-2010-
- http://www.dailykalerkantho.com/?view=details&archiev=yes&arch_date=13-022012&type=gold&data=Loan&pub_no=791&cat_id=1&menu_id=13&news_type_id=1&index=5
- http://nilakas-duronto.blogspot.com/2011/04/Digital Evidences Act-law-and-its-weakness-bangladesh.html
- http://support.microsoft.com/kb/129972
- http://en.wikipedia.org/wiki/Computer_virus
- http://www.Digital Evidences Actguards.com/Digital Evidences ActStalking.html
- http://en.wikipedia.org/wiki/Digital Evidences Actstalking
- http://www.dailykalerkantho.com/?view=details&archiev=yes&arch_date=13-022012&type=gold&data=Loan&pub_no=791&cat_id=1&menu_id=13&news_type_id=1&index=5