regulation mechanisms in human and machine systems, including computers.

Cyberpunk is a sensibility or belief that a few outsiders, armed with their own individuality and technological capability, can fend off the tendencies of traditional institutions to use technology to control society. The term, combining "cyber" and punk, possibly originated in 1980 with Bruce Bethke's short story, "Cyberpunk." An editor of Isaac Asimov's Science Fiction Magazine, Gardner Dozois, is credited with associating the word with a literary movement that includes the science fiction of William Gibson and Neal Stephenson.

The alt.cyberpunk.FAQ lists several categories of groups associated with cyberpunk:

a) hacker, who represent the best kind of cyberpunk

b) cracker, who attempt to break into computer systems

c) phreak, who attempt to break into telephone systems

d) Cypher-punks, who attempt to break codes and foil security systems

Cyberspace is the total interconnectedness of human beings through computers and telecommunication without regard to physical geography. William Gibson is sometimes credited with inventing or popularizing the term by using it in his novel of 1984, Neuromancer.

1.2. Definition of Cyber Law:

The ICT Act of Bangladesh does not define the Cyber law in any of the sections. Cyber law is fast evolving into its own discipline, and "traditional"

law firms are keen to enter the lucrative new legal area.[1] Cyber law is a generic term, which denotes all aspects, issues and the legal consequences on the Internet, the World Wide Web and cyber space.Cyber law is a term first coined by Jonathan Rosenoer as the title for a service aimed at explaining legal issues to computer users. It derives from the term, Cybernetics.[2]Cyber law (also referred to as Cyber law) describes the legal issues related to use of inter-networked information technology. It is less a distinct field of law in the way that property or contract are, as it is a domain covering many areas of law and regulation. Some leading topics include intellectual property, privacy, freedom of expression, and jurisdiction.[2]The area of law dealing with the use of computers and the Internet and the exchange of communications and information thereon, including related issues concerning such communications and information as the protection of intellectual property rights, freedom of speech, and public access to information.

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the Internet. There is no one exhaustive definition of the term "Cyber Law". Simply speaking, Cyber Law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web.

With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace began cropping up. In response to the absolutely complex and newly emerging legal issues relating to cyberspace, CYBERLAW or the law of Internet came into being. The growth of Cyberspace has resulted in the development of a new and highly specialised branch of law called Cyberlaws- Laws of The Internet & The World Wide Web.

There is no one exhaustive definition of the term "Cyber law". However, simply put, Cyber law is a term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to, or emanating from, any legal aspects or issues concerning any activity of netizens and others, in Cyberspace comes within the ambit of Cyber law.

---

1. Monica Kilian, "Cybersquatting and Trademark Infringement",

law firms are keen to enter the lucrative new legal area.[1] Cyber law is a generic term, which denotes all aspects, issues and the legal consequences on the Internet, the World Wide Web and cyber space.Cyber law is a term first coined by Jonathan Rosenoer as the title for a service aimed at explaining legal issues to computer users. It derives from the term, Cybernetics.[2]Cyber law (also referred to as Cyber law) describes the legal issues related to use of inter-networked information technology. It is less a distinct field of law in the way that property or contract are, as it is a domain covering many areas of law and regulation. Some leading topics include intellectual property, privacy, freedom of expression, and jurisdiction.[2]The area of law dealing with the use of computers and the Internet and the exchange of communications and information thereon, including related issues concerning such communications and information as the protection of intellectual property rights, freedom of speech, and public access to information.

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the Internet. There is no one exhaustive definition of the term "Cyber Law". Simply speaking, Cyber Law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web.

With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace began cropping up. In response to the absolutely complex and newly emerging legal issues relating to cyberspace, CYBERLAW or the law of Internet came into being. The growth of Cyberspace has resulted in the development of a new and highly specialised branch of law called Cyberlaws- Laws of The Internet & The World Wide Web.

There is no one exhaustive definition of the term "Cyber law". However, simply put, Cyber law is a term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to, or emanating from, any legal aspects or issues concerning any activity of netizens and others, in Cyberspace comes within the ambit of Cyber law.

1.5. Scope of Cyber Law:

Information society geared by development and convergence of computer, Telecommunication and broadcasting technologies – called, information and communication technologies (ICTs) – today destructively as well as creatively shifts paradigms of industries and life styles in many countries. There has been in tradition legislation designed to regulate various aspects of human activities. It used to be relatively easy for legislators to enact laws when a particular area of human activity needs to be regulated. Now, with the revolution of ICTs, it is not new activities per se but ways that people conduct their activities need to be regulated. Indeed, the ways of conducting human activities have substantially changed with the advent of technological revolution especially in the information or cyber era.

Bangladesh has enacted the first cyberlaw to foster the advantages of new technologies - i.e., ICTs - as well as to tackle some of the emerging issues on cyber-activities or crimes. For instance, the Act proposes facilitation of:

- Electronic commerce transactions;
- Maintenance of electronic records; and
- Electronic government transactions.

The Act also provides for a legal framework for *validation of information in electronic form* and deals with the major issues as follows, but not limited to: e.g.,

- **Securing electronic transactions**: These enable parties to enter into electronic contracts.
- **Attribution of electronic messages**: i.e., Once the message leaves the information system of the originator of the message, it is attributed to him.
- **Electronic signatures and electronic records given legal status**. In furtherance of this, and to maintain security of information, the Act establishes a Digital Signature Infrastructure making specific use of the Asymmetric Crypto System Technology with new authorities such as the Controller of Certifying Authorities being set up.
- **'Contraventions'** regarding electronic records vis. hacking theft of electronic records, manipulation of records, spreading viruses, etc. have been defined. Involved in the inquiry and determination of the result of the proceeding is an adjudicating officer, appointed by the Government and possessing wide-ranging powers.
- Information Technology Offences viz. tampering with computer source documents - i.e., **obscenity.** A limited number of offences have been created under the Act. These will be tried as any other criminal offences, which are

under the Criminal Procedure Code but with unique provisions for investigation, search, etc., provided in the Act.

- **Right of government bodies** to decrypt information has been specifically given herein.

- **Privacy and confidentially of information** submitted to statutory authorities. Dissemination to third parties of such information collected in pursuance of powers under the Act is made a criminal offence.

- **Facilitates e-commerce** as well as **electronic filing and maintenance of records** as against the government.

Setting up of **new authorities/regulatory infrastructure:** e.g., cyber regulatory authorities such as the controller of Certifying Authorities and the Cyber Regulations Appellate Tribunal (CRAT) have been established. The Act also seeks to set up a Cyber Regulations Advisory Committee (CRAC).

Liability of Internet Services Providers for content on the Internet is limited in so far as the provider exercises all due diligence. This is relevant in connection with copyright violations, pornography, etc., residing on various web pages or moving through the systems of the ISP.

1.6. Advantages of Cyber Law:

The Information and Communication Technology Act, 2006 attempts t change outdated laws and provides ways to deal with cyber crimes. We nee such laws so that people can perform purchase transactions over the Ne through credit cards without fear of misuse. The Act offers the much-neede

or computer network; ...manipulating any computer, computer system

Then the Act of that person shall be considered to be a crime under this Act.

2.15. Meaning of Computer Contaminant:

As per Section 54 of the ICT Act, computer contaminant means any set of computer instructions that are designed to modify, destroy, record, transmit data or programme residing within a computer, or by any means to usurp the normal operation of the computer, computer system, or computer network.

Explanation of Section 54 of the ICT states that for the purposes of this section,-

"Computer contaminant" means any set of computer instructions that are designed-

(a) To modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) By any means to usurp the normal operation of the computer, computer system or computer network;

2.16. Meaning of Computer Database:

Databases play an important role in the development of information market and its products. A large number of databases are available online from foreign vendors which are finding an increasing market in the country. Over the past few years, Bangladesh is gradually building up capability in the database field and initiatives are taken by domestic vendors and institutions to commercialise databases and related services in a number of fields. The vast expertise and capabilities in ... that are available in the ...

ous to Bangladeshi IP jurisprudence, that country has addressed itself
es arising from sui generis database protection in recent years.[27]

2.17. Meaning of Computer Virus:

Virus is a program that attaches itself to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

Explanation of Section 54 of the ICT defines "Computer Virus" as an computer instruction, information, data or programme that, destroy damages, degrades or adversely affects the performance of a compu

---

[27] Apar Gupta, "Protection ofdatabases in India and *sui generis* protection", *Journal of Intellectual Property Law &PrActice*, July: 2007, Oxford University Press.

programme, data or instruction is executed or some other event takes place in that computer resource.

In the United States alone, the virus made its way through 1.2 millio computers in one-fifth of the country's largest businesses. David Smith pleade guilty on Dec. 9, 1999 to state and federal charges associated with his creatio of the Melissa virus. There are numerous examples of such computer virus few of them being "Melissa" and "love bug". The Melissa virus first appear on the internet in March of 1999. It spread rapidly throughout compu systems in the United States and Europe. It is estimated that the virus cau 80 million dollars in damages to computers worldwide.

2.18. Meaning of Damage of Computer:

Explanation of Section 54 of the ICT defines "damage" as to destroy, a delete, add, modify or re-arrange any

programme, computer system or computer network, when the computer source code is required to be kept or maintained by any law for the time being in force, shall be punishable. If any person does a crime under subsection 1 of the section he will be given imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka three lacs, or with both. This section provides for computer source code. Thus protection has been provided against tampering of computer source documents.

2.20. Meaning of Computer Source Code:

Explanation of Section 55 of the ICT defines "computer source code" as the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Malaysia. Where a computer crime is committed outside Malaysia in respect of computers or data in Malaysia or that which may be connected to or used in Malaysia, the crime may be treated as a crime within Malaysia and the perpetrator may be dealt with under the provisions of this Act.[6]

But there is disagreement nationally and globally as to what exactly constitutes a computer crime.[7] The term "computer crime" covers such a wide range of offenses that unanimity has been an elusive goal. For example, if a commercial burglary takes place and a computer is stolen, does this constitute a computer crime, or is it merely another burglary? Does copying a friend's Microsoft Excel disks constitute a computer crime? What about sending obscene pictures over the Internet? The answers to each of these questions may depend entirely upon the jurisdiction in which one finds oneself.[8]

12.5. Meaning and definition of Cyber Crime:

As regards exact definition of cybercrimes, it has not been statutorily defined in any statute or law as yet. Even ***the Information & Communication Technology Act*** (ICT), ***2006*** does not contain the definition of cybercrime. However, cybercrimes may precisely be said to be those species of crime in which computer is either an object or a subject of conduct constituting the crime or it may be even both. Thus, any activity that uses computer as an instrumentality, target or a means for perpetrating further crime, falls within the ambit of cybercrime.

Prof. S.T. Viswanathan has given 3 possible definitions of cyber crimes and these are as follows:

---

legalserviceindia.com/articles/articles.html>

a. Any illegal action in which a computer is the tool or objects of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,

b. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,

c. Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic

18.1. Hackers:

"Hacker"[1] is a term commonly applied to a "computer user who intends to gain unauthorized access to a computer system."[2] Hackers are skilled computer users who penetrate computer systems to gain knowledge about computer systems and how they work.[3] The traditional hacker does not have authorized access to the system.[4] Hacking purists do not condone damage to the systems that are hacked.[5] According to The Jargon Dictionary, the term "hacker" seems to have been first adopted as a badge in the 1960s by the hacker culture surrounding The Tech Model Railroad Club ("TMRC") at Massachusetts Institute of Technology when members of the group began to work with computers.[6] The TMRC resents the application of the term "hacker" to mean the committing of illegal acts, maintaining that words such as "thieves," "password crackers," or "computer vandals" are better descriptions.[7]

In the hacking "community," it is considered better to be described as a "hacker" by others than to describe oneself as a "hacker."[8] Hackers

1. Access to computers should be unlimited and total.

2. All information should be free.

3. Mistrust authority—promote decentralization.

4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position.

---

1. 10. The term "hacker" has been defined 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." WEBSTER'S NEW WORD DICTIONARY OF COMPUTER TERMS 235 (7th ed. 1999). *See* Appendix A for a more detailed definition.
2. Michael P. Dierks, *Symposium: Electronic Communications and Legal Change, Computer Network Abuse*, 6 HARV. J. L. & TECH. 307, 310 n.7 (1993).
3. According to Deb Price and Steve Schmadeke, the "Hackers credo" is:
4. However, this is not a legal distinction. The Computer Fraud and Abuse Act criminalizes unauthorized access and access that exceeds authorization. *See* 18 U.S.C.A. § 1030(a)(1) (West Supp. 1999).
5. *See* Dissident, *Ethics of Hacking* (visited Mar. 3, 2000) <http://cultdeadbunnies.virtualave.net/hacking/lit/files/ethics.txt>.
6. *See* The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/h.html#hacker>.
7. *See generally* STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION (1984).
8. *See* Appendix A.

computer users who penetrate computer systems to gain knowledge about computer systems and how they work.[3] The traditional hacker does not have authorized access to the system.[4] Hacking purists do not condone damage to the systems that are hacked.[5] According to The Jargon Dictionary, the term "hacker" seems to have been first adopted as a badge in the 1960s by the hacker culture surrounding The Tech Model Railroad Club ("TMRC") at Massachusetts Institute of Technology when members of the group began to work with computers.[6] The TMRC resents the application of the term "hacker" to mean the committing of illegal acts, maintaining that words such as "thieves," "password crackers," or "computer vandals" are better descriptions.[7]

In the hacking "community," it is considered better to be described as a "hacker" by others than to describe oneself as a "hacker."[8] Hackers

1. Access to computers should be unlimited and total.

2. All information should be free.

3. Mistrust authority—promote decentralization.

4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position.

---

1. 10. The term "hacker" has been defined 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." WEBSTER'S NEW WORD DICTIONARY OF COMPUTER TERMS 235 (7th ed. 1999). *See* Appendix A for a more detailed definition.
2. Michael P. Dierks, *Symposium: Electronic Communications and Legal Change, Computer Network Abuse*, 6 HARV. J. L. & TECH. 307, 310 n.7 (1993).
3. According to Deb Price and Steve Schmadeke, the "Hackers credo" is:
4. However, this is not a legal distinction. The Computer Fraud and Abuse Act criminalizes unauthorized access and access that exceeds authorization. *See* 18 U.S.C.A. § 1030(a)(1) (West Supp. 1999).
5. *See* Dissident, *Ethics of Hacking* (visited Mar. 3, 2000) <http://cultdeadbunnies.virtualave.net/hacking/lit/files/ethics.txt>.
6. *See* The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/h.html#hacker>.
7. *See generally* STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION (1984).
8. *See* Appendix A.

Chapter–18
HACKING & CYBER LAW

18.1. Hackers:

"Hacker"[1] is a term commonly applied to a "computer user who intends to gain unauthorized access to a computer system."[2] Hackers are skilled computer users who penetrate computer systems to gain knowledge about computer systems and how they work.[3] The traditional hacker does not have authorized access to the system.[4] Hacking purists do not condone damage to the systems that are hacked.[5] According to The Jargon Dictionary, the term "hacker" seems to have been first adopted as a badge in the 1960s by the hacker culture surrounding The Tech Model Railroad Club ("TMRC") at Massachusetts Institute of Technology when members of the group began to work with computers.[6] The TMRC resents the application of the term "hacker" to mean the committing of illegal acts, maintaining that words such as "thieves," "password crackers," or "computer vandals" are better descriptions.[7]

In the hacking "community," it is considered better to be described as a "hacker" by others than to describe oneself as a "hacker."[8] Hackers

1. Access to computers should be unlimited and total.
2. All information should be free.
3. Mistrust authority—promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position.

---

1. The term "hacker" has been defined 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." WEBSTER'S NEW WORD DICTIONARY OF COMPUTER TERMS 235 (7th ed. 1999). See Appendix A for a more detailed definition.
2. Michael P. Dierks, *Symposium: Electronic Communications and Legal Change, Computer Network Abuse*, 6 HARV. J. L. & TECH. 307, 310 n.7 (1993).
3. According to Deb Price and Steve Schmadeke, the "Hackers credo" is: "However, this is not a legal distinction. The Computer Fraud and Abuse Act criminalizes unauthorized access and access that exceeds authorization. *See* 18 U.S.C.A. § 1030(a)(1) (West Supp. 1999).
4. Dissident, *Ethics of Hacking* (visited Mar. 3, 2000) <http://www.[illegible].net/hacking/lit/files/ethics.txt>.
5. [illegible] (visited Mar. 9, 2000)
6. [illegible] REVOLUTION (1984).

markup language ("HTML") is code that will cause the person's e-mail program to send an e-mail to the web site with the person's e-mail in the "from" slot. Theoretically, this exploit would allow a web site to collect all of the e-mails from persons who visit their web site. Internet Explorer and Netscape Navigator provide security warnings to users before they send the mail if the security level is set at a higher level.

18.2. Hacking with Computer System:

Hacking is usually understood to be the unauthorized access of a computer system and networks. Originally, the term "hacker" describes any amateur computer programmer who discovered ways to make software run more efficiently. Hackers usually "hack" on a problem until they find a solution, and keep trying to make their equipment work in new and more efficient ways. A hacker can be a Code Hacker, Cracker or a Cyber Punk. Protection against hacking has been provided under section 56. As per this section hacking is defined as any Act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss of damage will be caused to any person and information residing in a computer resource must be either destroyed, deleted, altered or its value and utility get diminished.

Section 56(1) of the ICT Act, 2006 provides that if whoever, (a) With the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (b) 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".

18.3. Punishment of Hacking with Computer System:

Section 56(2) imposes the penalty of imprisonment of three years or fine up to Taka one crore or both on the hacker. According to section 56(2) of

---

Collecting Data on Users of its Internet Software, Provoking the First Class Actions in Such a Case, L.A. TIMES, Nov. 11, 1999 at C1.

[40] *See DigiCrime E-mail Address Demonstration* (visited Mar. 5, 2000). <http://www.digicrime.com/noprivacy.html> (copy on file with the author). *See also Onion Routing* (visited Mar. 5, 2000) <http://www.onion-router.net/Tests.html> (listing other good privacy testing sites).

5. You can create art and beauty on a computer.

6. Computers can change your life for the better.

Deb Price & Steve Schmadeke, *Hackers Expose Web Weakness: There's No Defense Against Internet Assaults, Experts Confess, and Attackers are Elusive*, DET. NEWS, Feb. 14, 2000 at A1, *available in* 2000 WL 3467302. consider themselves members of an elite meritocracy based on ability and trade hacker techniques and "war stories" amongst themselves in Usenet forums, local or regional clubs, and national conferences, such as the annual Def Con Computer Underground Convention held in Las Vegas.[9]

2. Crackers

A "cracker" is a hacker with criminal intent.[10]19 According to The Jargon Dictionary,[11] the term began to appear in 1985 as a way to distinguish "benign" hackers from hackers who maliciously cause damage to targeted computers. Crackers[12] maliciously sabotage computers, steal information located on secure computers, and cause disruption to the networks for personal or political motives.[13]

Estimates made in the mid-1990's by Bruce Sterling, author of *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, put "the total number of hackers at about 100,000, of which 10,000 are dedicated and obsessed computer enthusiasts. A group of 250-1,000 are in the so-called hacker 'elite', skilled enough to penetrate corporate systems and to unnerve corporate security."[14]

---

[9]. DEF CON is an annual computer underground party and conference for hackers held every summer in Las Vegas, Nevada. *See* DEF CON (visited Apr. 5, 2000) <http://www.defcon.org>.

[10] The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/c/cracker.html>.

[11] *See* Appendix A.

[12] Please note that a "cracker" is different from a "crack." A crack is a script that defeats software protection [illegible] that allows

...ICT Act, 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.

18.4. Crime and punishment for unauthorised acces to protected system:

This activity is commonly referred to as hacking. The Bangladeshi ICT law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Act of 2006 is much wider than hacking.

18.5. How does ICT Act deal with hacking>

ICT Act defines hacking as [Section 56] "Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking". Further for the first time, punishment for unauthorized access as a cyber crime is prescribed in the form of imprisonment upto 10 years or with fine that may extend to Taka one crore or with both. On the other hand, punishment for hacking as a cyber crime is prescribed in the form of imprisonment upto 3 years or with fine that may extend to Taka 10 lacs or with both under section 61 of the ICT Act. According to section 61 of the ICT Act, the controller may, by notification in the Government Official Gazette or willingly in electronic gazette declare any computer, computer system or computer network to be a protected system. Even that if any person enters into those computer, computer system, or computer network illegally then it will be considered as a crime. If any person does any crime under sub-section 1 of the section he shall be punished with imprisonment of either description for a term which may extend to ten years or with fine which may extend to Taka 10 lacs or with both.[41]

the ICT Act, 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.

18.4. Crime and punishment for unauthorised acces to protected system:

This activity is commonly referred to as hacking. The Bangladeshi ICT law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Act of 2006 is much wider than hacking.

18.5. How does ICT Act deal with hacking>

ICT Act defines hacking as [Section 56] "Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking". Further for the first time, punishment for unauthorized access as a cyber crime is prescribed in the form of imprisonment upto 10 years or with fine that may extend to Taka one crore or with both. On the other hand, punishment for hacking as a cyber crime is prescribed in the form of imprisonment upto 3 years or with fine that may extend to Taka 10 lacs or with both under section 61 of the ICT Act. According to section 61 of the ICT Act, the controller may, by notification in the Government Official Gazette or willingly in electronic gazette declare any computer, computer system or computer network to be a protected system. Even that if any person enters into those computer, computer system, or computer network illegally then it will be considered as a crime. If any person does any crime under sub-section 1 of the section he shall be punished with imprisonment of either description for a term which may extend to ten years or with fine which may extend to Taka 10 lacs or with both.[41]

21.1. Establishment of Cyber Appellate Tribunal:

What have so far escaped the public eye are the provisions relating to the Cyber Appellate Tribunal (CAT) and more specifically, its composition. The ICT Act envisages the establishment of CATs at one or more places as the Government may deem fit. Section 82(1) of the Act provides that the Government shall, by notification in the Official Gazette, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal. The cyber appeal tribunal will be comprised of a chairman and two members appointed by the government.[2] The chairman will be such a person, who was a justice of the Supreme Court or is continuing his post or capable to be appointed as such and one of the members will be as an appointed judicial executive as a district judge or he may be retired and the other will be a person having the knowledge and experience in information and technology that is prescribed.[3] The chairman and the members will be in their post minimum 3 years and maximum 5 years and the conditions of their service will be decided by the government.[4]

21.2. Procedure and powers of Cyber Appellate Tribunal:

The Cyber Appellate Tribunal shall have the power to here and settle the appeal made against the judgment of cyber tribunal and session court.[5] In case of hearing and settling any appeal, the cyber appeal tribunal will follow the rules made there under and if the procedure is not fixed by making rules, those rules with proper adoption will be followed which the high court division follow in case of criminal justice by the appeal tribunal.[6] The appeal tribunal will have the authority of supporting, canceling, changing or editing the judgment of the cyber tribunal.[7] The decision of the appeal tribunal will be final.[8] Under this part of the Act if the Cyber Appeal Tribunal is not established, whatever may be in the Code of Criminal Procedure appeal may be made to high court division of the Supreme Court

Chapter–21
CYBER APPELLATE TRIBUNAL

21.1. Establishment of Cyber Appellate Tribunal:

What have so far escaped the public eye are the provisions relating to the Cyber Appellate Tribunal (CAT) and more specifically, its composition. The ICT Act envisages the establishment of CATs at one or more places as the Government may deem fit. Section 82(1) of the Act provides that the Government shall, by notification in the Official Gazette, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal. The cyber appeal tribunal will be comprised of a chairman and two members appointed by the government.[2] The chairman will be such a person, who was a justice of the Supreme Court or is continuing his post or capable to be appointed as such and one of the members will be as an appointed judicial executive as a district judge or he may be retired and the other will be a person having the knowledge and experience in information and technology that is prescribed.[3] The chairman and the members will be in their post minimum 3 years and maximum 5 years and the conditions of their service will be decided by the government.[4]

21.2. Procedure and powers of Cyber Appellate Tribunal:

The Cyber Appellate Tribunal shall have the power to here and settle the appeal made against the judgment of cyber tribunal and session court.[5] In case of hearing and settling any appeal, the cyber appeal tribunal will follow the rules made there under and if the procedure is not fixed by making rules, those rules with proper adoption will be followed which the high court division follow in case of criminal justice by the appeal tribunal.[6] The appeal tribunal will have the authority of supporting, canceling, changing or editing the judgment of the cyber tribunal.[7] The decision of the appeal tribunal will be final.[8] Under this part of the Act if the Cyber Appeal Tribunal is not established, whatever may be in the Code of Criminal Procedure appeal may be made to high court division of the Supreme Court

---

2. Section 82(2), the ICT Act, 2006.
3. Section 82(3), the ICT Act, 2006.
4. Section 82(4), the ICT Act, 2006.
5. Section 83(1), the ICT Act, 2006.
6. Section 83(2), the ICT Act, 2006.
7. Section 83(3), the ICT Act, 2006.
8. Section 83(4), the ICT Act, 2006.

The jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof.[1] A Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two members of such Tribunal as the Chairperson may deem fit.[2] The Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, specify by notification in the Official Gazette. [3][31] By notification in the Official Gazette, the Central Government shall specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.[4]

The Chairperson of the Cyber Appellate Tribunal may transfer a member of such Tribunal from one Bench to another Bench.[5]

If at any stage of the hearing of any case or matter it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, then the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.[6]

3. Qualification for appointment as Chairperson and Members of Cyber Appellate Tribunal

A person can be appointed as a Chairperson of the Cyber Appellate Tribunal if he is, or has been, or is qualified to be, a Judge of a High Court.[7]

The Members of the Cyber Appellate Tribunal, except the Judicial Member, shall be appointed by the Central Government from amongst persons, having special knowledge of, and professional experience in, information technology, telecommunication, industry, management or consumer affairs.[8]

A person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than 1 year, or Joint Secretary to the Government of India or any

---

1. *Ibid.*, Section 49 (3) (a
2. *Ibid.*, Section 49 (3) (b)
3. *Ibid.*, Section 49 (3) (d)
4. *Ibid.*, Section 49 (3) (d)
5. *Ibid.*, Section 49 (4)
6. *Ibid.*, Section 49 (5)
7. *Ibid.*, Section 50 (1).
8. *Ibid.*, Section 50 (2)

safeguards are contained in the enactment to ensure that he possesses the requisite legal qualifications, it is still doubtful whether such presiding officer would possess the technological expertise and knowledge which is to be harmonized with the legal knowledge for resolving ICT related disputes. It would therefore have been ideal for the CAT to comprise of at least one judicial member and one technical member (with a computer science background) to effectively hear and resolve disputes before it. The omission of a technical member is all the more glaring since several tribunals/quasi judicial bodies like the Income Tax Appellate Tribunal, Sales Tax Tribunal, Central Administrative Tribunal, Company Law Board, Board for Industrial and Financial Reconstruction etc. have departmental members who assist the Presiding Officer or the judicial member in resolving the disputes. Considering the fact that the case laws with respect to Information and Communication Technology are almost non-existent in our country and the decisions of the Cyber Appellate Tribunal are going to be trend setting, it is still not too late for the Government to consider amending the ICT Act and providing that the CAT comprise of one technical member as well, which undoubtedly, is going to go a long way in ensuring that the correct concepts of Information Technology are applied while resolving ICT disputes.

21.3. Cyber Appellate Tribunal:

1. Establishment of Cyber Appellate Tribunal

The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.[2]125

The Central Government shall also specify in the notification, the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.[3]

2. Composition of Cyber Appellate Tribunal

The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other members, as the Central Government may, by notification in the Official Gazette, appoint.[4]

The selection of Chairperson and members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.[5]

---

[2] *Ibid*., Section 48 (1)
[3] *Ibid*., Section 48 (2)
[4] *Ibid*., Section 49 (1)
[5] *Ibid*., Section 49 (2)

against judgments of session judges or Cyber Tribunal.[1] These Tribunals are placed lower in hierarchy to the High Courts and higher in hierarchy to the "adjudicating officer" The primary function of an "adjudicating officer" would be to hold an inquiry into whether any person has contravened the provisions of the ICT Act and impose penalty accordingly. Although the CAT 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,

(a) summoning and examination of witnesses

(b) requiring production of documents

(c) receiving evidence

(d) issuing commissions and

(e) reviewing its decisions.

Typically, such powers are vested in a judicial body having original jurisdiction. Therefore, by being juxtaposed between the High Court and the "adjudicating officer", the CAT would be both, an appellate authority as well as a fact finding authority, whose function would be to determine whether the provisions of the ICT Act have been contravened. Interestingly, the Act provides that the Tribunal shall consist of one person only (presiding officer) who is qualified to be a High Court judge or a member of the Bangladeshi Legal Services holding a Grade I post. Apart from the factual issues that would be raised, the disputes before the CAT are invariably going to involve the following legal issues as well:

(a) application of Private International Law (including the issue of "conflict of laws") in case the parties to the dispute belong to different nationalities;

(b) issues regarding jurisdiction; and

(c) application and interpretation of complex contractual, intellectual property and penal laws

Since the above issues are to be resolved vis-a-vis the laws pertaining to Information Technology, one would also need an in-depth knowledge of computer applications in the field of information technology. It is essential for the Tribunal to understand the technical aspects pertaining to digital signatures, cryptography etc. apart from keeping abreast with the latest developments in the field of Information Technology. While one cannot call into question the legal acumen of the presiding officer, as adequate

equivalent post in the Central Government or State Government for a period of not less than 7 years.[9]

The Judicial Member of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than 1 year or Grade I post of that service for a period of not less than 5 years.[10]

4. Term of office, conditions of service, etc., of Chairperson and Members The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of 5 years from the date on which he enters upon his office or until he attains the age of 65 years, whichever is earlier.[11]

Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.[12]

An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, shall have to ret... from service before joining as such Chair...

7. Distribution of business among Benches

Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench. [1]

8. Power of Chairperson to transfer cases

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or *suo motu* without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench for disposal to any other Bench.[2]

9. Decision by majority

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.[3]

10. Filling up of vacancies

If, for reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or Member of a Cyber Appellate Tribunal, then the Central Government shall appoint another person to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled. [4]

11. Resignation and removal

The Chairperson or Member of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office.[5]

However, the said presiding officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of 3 months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest. [6]

The presiding officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground

of proved misbehavior or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.[7]

The Central Government may, by rules, regulate the procedure for the investigation of misbehavior or incapacity of the aforesaid Presiding Officer.[8]

12. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings

No order of the Central Government appointing any person as the Chairperson or Member of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.[9]

13. Staff of the Cyber Appellate Tribunal

The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.[10]

The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Chairperson.[11]

The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.[12]

14. Appeal to Cyber Appellate Tribunal

Any person aggrieved by an order made by the controller or an adjudicating officer under the IT act, 2000 may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.[13]

No appeal against order made with the consent of parties

No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.[14]

---

7. *Ibid.*, Section 54 (2)
8. *Ibid.*, Section 54 (3)
9. *Ibid.*, Section 55
10. *Ibid.*, Section 56 (1)
11. *Ibid.*, Section 56 (2)
12. *Ibid.*, Section 56 (3)
13. *Ibid.*, Section 57 (1)

Chapter–20
CYBER TRIBUNAL

20.1. Establishment of Cyber Tribunal:

Government of Bangladesh by gazette notification, for the purpose of quick and effective trial of the crimes committed under the Act, may establish one or more cyber tribunal, sometimes which is stated later as tribunal under section 68(1) of the ICT Act. The cyber 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 consultation with the supreme court; and such a judge appointed will be introduced "judge, cyber tribunal".[1] The cyber tribunal under the section may be given jurisdiction of whole Bangladesh or one or more session jurisdiction; and the tribunal will only judge the cases of crimes under the Act.[2] The special tribunal may sit and continue its procedure on a place at a certain time and government will dictate all this by its order.[3]

20.2. Procedure of trial of the Cyber Tribunal:

rding to section 69(1) of the ICT Act, the special tribunal will not trial unless there is a written report by any police officer of sub-inspector and approval of the controller or such rity from the controller for the purpose. The tribunal Act will follow chapter 23 of the Code of Criminal ession court; provided that it will not be contradictory tribunal for the purpose of justice if considered istering it can not stop the proceedings of a case.[5] believe for the tribunal that, the accused person is for which it is not possible to arrest him or there is m earlier, in that case the tribunal, by its order, t in the court by publishing it in two prominent bed time and if that person fails to do so, the The accused person or the person having if he fails to

a. Summoning and enforcing the attendance of any person and examining him on oath;

b. Requiring the discovery and production of documents or other electronic records;

c. Receiving evidence on affidavits;

d. Issuing commissions for the examination of witnesses or documents;

e. Reviewing its decisions;

f. Dismissing an application for default or deciding it *ex parte*;

g. Any other matter which may be prescribed.[7]

iii. Proceedings of the Cyber Appellate Tribunal

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of Sections 193 and 228 and for the purposes of Section 196 of the Indian Penal Code, 1860, and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of Section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.[8]

16. Right to legal representation

The appellant may either appear in person or authorize one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.[9]

17. Limitation Period

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.[10]

18. Civil court not to have jurisdiction

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by this Act.[11]

19. Appeal to high court

---

[7] *Ibid.*, Section 58 (2)
[8] *Ibid.*, Section 58 (3)
[9] *Ibid.*, Section 59
[10] *Ibid.*, Section 60

ii. Limitation period for filing an appeal

Every appeal shall be filed within a period of 45 days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed [1]

However, the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of 45 days if it is satisfied that there was sufficient cause for not filing it within that period. [2]

iii. Order of the Cyber Appellate Tribunal

On receipt of an appeal, the Cyber Appellate Tribunal may, after giving the parties to appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against. [3]

iv. Copy of the order

The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer. [4]

v. Limitation period for deciding an appeal

The appeal filed before the Cyber Appellate Tribunal shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within 6 months from the date of receipt of the appeal. [5]

15. Procedure and powers of the Cyber Appellate Tribunal

i. Procedure of the Cyber Appellate Tribunal

The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to the other provisions of the IT Act, 2000 and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings. [6]

ii. Powers of the Cyber Appellate Tribunal

For the purposes of discharging its functions under the IT Act, 2000, the Cyber Appellate Tribunal shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:

20.1. Establishment of Cyber Tribunal:

Government of Bangladesh by gazette notification, for the purpose of quick and effective trial of the crimes committed under the Act, may establish one or more cyber tribunal, sometimes which is stated later as tribunal under section 68(1) of the ICT Act. The cyber 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 consultation with the supreme court; and such a judge appointed will be introduced "judge, cyber tribunal".[1] The cyber tribunal under the section may be given jurisdiction of whole Bangladesh or one or more session jurisdiction; and the tribunal will only judge the cases of crimes under the Act.[2] The special tribunal may sit and continue its procedure on a place at a certain time and government will dictate all this by its order.[3]

20.2. Procedure of trial of the Cyber Tribunal:

According to section 69(1) of the ICT Act, the special tribunal will not take any case for trial unless there is a written report by any police officer not under the rank of sub-inspector and approval of the controller or such person having authority from the controller for the purpose. The tribunal during trial under the Act will follow chapter 23 of the Code of Criminal Procedure for trial in session court; provided that it will not be contradictory with this Act.[4] Any tribunal for the purpose of justice if considered unnecessary without registering it can not stop the proceedings of a case.[5] Where there is reason to believe for the tribunal that, the accused person is missing or hiding himself for which it is not possible to arrest him or there is less possibility to arrest him earlier, in that case the tribunal, by its order, may ask that person to present in the court by publishing it in two prominent Bangle newspaper at a prescribed time and if that person fails to do so, the trial will held with his absence.[6] The accused person or the person having bail, after being present before the tribunal, if he is missing, or if he fails to

---

1. Section 68(2) of the ICT Act, 2006.
2. Section 68(3) of the ICT Act, 2006.
3. Section 68(4) of the ICT Act, 2006.
4. Section 69(2) of the ICT Act, 2006.
5. Section 69(3) of the ICT Act, 2006.
6. Section 69( ) of the ICT Act, 2006.

present in front of the tribunal, the process stated in sub-section (4), will not be applicable, and that tribunal with absence of that person, try him registering its decision.[7] If the person having bail or after presenting the court, fails to present before the court the procedure stated in sub-section 4 of the section shall not be applied and the tribunal may in written form give judgement without the presence of the accused.[8] The tribunal on the basis of the application presented before it, or by its own effort, give the order to reinvestigate any case made under the Act and give the order to submit report in a prescribed time by the authority to any police official, or in cases any person having the authority from the controller.[9]

20.3. The Application of Criminal Procedure in the procedure of the Tribunal:

According to section 70 of the ICT Act, the laws of the Criminal Procedure, as far as possible, being not contrary to this Act will be applicable to the procedure of the tribunal and the tribunal will have all the original jurisdiction of the session judge. The advocate on behalf of the government shall be known as the public prosecutor.

20.4. Bail Rules:

According to section 71 of the ICT Act, the judge of the Cyber Tribunal will not give bail to any person accused under the Act, unless-

(a) The government side is given scope for hearing on the grounds of bail:

(b) The judge is satisfied that- (i) There is enough ground to believe that the accused might not be proved guilty; (ii) The crime in prima facie view is not too heavy and the punishment, even the crime is proved, will not be hard.

(c) He registers all those satisfactory grounds in written form.

20.5. The time limit to give Judgment:

According to section 72(1) of the ICT Act, the judge of the tribunal from the date of finishing examination of witness or evidence or hearing, whichever occurs later, will give judgment within ten days if he does not extend the time not more than ten days with written reasons for that. When judgment is given under subsection 1 of the section or if any appeal to cyber appeal tribunal is made against the judgment then the copy of the appeal judgment will be sent to the Controller by the Cyber Tribunal or

---

[7] of the ICT Act, 2006.

Appeal Tribunal to reserve it according to the section 18(7) of the Act; if such any copy is sent, the controller will take proper Action to reserve it with proper process.[1]

20.6. The time limit of disputing a case by the Tribunal:

According to section 73(1) of the ICT Act, the judge of the tribunal will complete the judgment procedure within 6 months of filing the case. If the judge fails to finish the case within the time prescribed under sub-section 1 of the section, he may increase the time limit not more than 3 months by stating written reasons.[2] If the judge fails to finish a case within the time limit under sub-section 2 of the section, he may continue the process by submitting a paper to high court and the controller stating the reasons behind the delay.[3]

20.7. Justice by Session Court:

According to section 74 of the ICT Act, whatever may be in the Code of Criminal Procedure, unless special tribunal is formed, the crimes made under the Act shall be judged under session judge. Under section 75 of the ICT Act, following procedures to be followed by the session judge:

- The session court will follow the section 23 of the Code of Criminal Procedure while judging the crimes under this Act.
- Whatever there may be in the Code of Criminal Procedure, without the report of any official having the status not less than a sub-inspector and any prior approval of any official appointed by the controller for the purpose any session court as its original jurisdiction, will not take any case to judge.

20.8. The power of investigation of crime etc.:

According to section 76(1) of the ICT Act, 2006, whatever may be in the code of criminal procedure, controller or any official having authority from the controller or any police official having the rank not less than the sub-inspector will investigate the crimes under the Act.

20.9. Are Cyber Crimes considered as cognizable or non-cognizable?

According to section 76(2) of the ICT Act, 2006, the crimes under this Act shall be considered as non-cognizable.

---

1. Section 72(2) of the ICT Act, 2006.
2. Section 73(2) of the ICT Act, 2006.
3. Section 73(3) of the ICT Act, 2006.

15) **"subscriber"** means a person in whose name the Digital Signature Certificate is issued;

16) **"Cchairman"** means a chairman appointed under cyber appeal tribunal of section 82 of this Act;

17) **"Civil Procedure"** means Code of Civil Procedure, 1908 (Act V 0f 1908);

18) **"Penal Code"** means Penal Code, 1860 (Act XLV of 1860);

19) **"prescribed"** means prescribed by rules;

20) **"secure signature generating machine or technology"** means any signature generating machine or technology subject to the conditions illustrated under section 17;

21) "Controller" or "Sub-Controller" or "Assistant Controller" means a Controller or Sub-Controller or Assistant Controller appointed under section 18(1);

22) **"addressee"** with reference to data message means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

23) **"verification"** means such procedure used to identify signatory or authentication of data message;

24) **"originator"** with reference to data message means a person who sends or prepares data message before preservation or causes any date message to be sent, generated, stored or transmitted but does not include an intermediary;

25) **"regulation"** means regulation prepared under this Act;

26) **"Criminal Procedure"** means Code of Criminal Procedure, 1898 (Act V of 1898);

27) **"person"** relates to unique person having any natural entity, partnership business, union, company, body corporate, cooperatives;

28) **"adjudicating officer"** means an adjudicating officer of cyber tribunal constituted under section 68 of this Act;

29) **"rule"** means rule prepared under this Act;

30) **"medium"** means any person sending, receiving, advancing or saving any data message or any service rendering on this data message on behalf of any other person for a particular data message;

31) **"licence"** means a licence granted under section 22 of this Act;

32) **"authentication service provider"** means certificate issuing [illegible] related to digital signature.

...ter memory, microfilm, ... similar ... or technology;

6) "**electronic gazette**" means the official gazette published in the electronic form in addition to official printed & published gazette;

7) "**electronic record**" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche;

8) "**internet**" means such an international computer network by which users of computer,cellular phone or any other electronic system around the globe can communicate with one another and interchange information and can browse the information presented in the websites;

9) "**electronic mail**" means information generated electronically and transmitted using internet;

10) "**data**" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner,and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and may be in any form including computer printouts, magnetic or optical storage media, punch cards, punched tapes or stored internally in the memory of the computer;

11) "**data message**" means electronic, electronic data interchange including optical, electronic mail, telegram, telex, fax, telecopy, short message or created something similar, sent, received or stored information;

12) "**website**" means document and information stored in computer and web server which can be browsed or seen by the user through internet;

13) "**computer**" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetical and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

14) "**computer network**" means the interconnection of one or more computers through the use of satellite, microwave, terrestrial line, wireless equipment, wide area network, local area network, infrared, WiFi, bluetooth or other communication media; and terminals or a complex consisting of two or more interconnected computers whether or not the ... is continuously maintained;

INFORMATION AND TECHNOLOGY ACT, 2006

[ACT NO. 39 OF 2006]

[WITH IT (AMDT.) ACT, 2013]

[October 8, 2006]

Act prepared to provide legal recognition and security of Informa-tion and Communication Technology and rules of relevant subjects

Since it is plausible and necessary to provide legal recognition and security of Information & Communication Technology and prepare rules of relevant subjects;

Thus hereby the following Act has been created:--

Chapter–1
Preliminary

1. Short title, extent and commencement: 1) This Act may be called the Information & Communication Technology Act, 2006.

2) It shall extend to the whole of Bangladesh.

3) It shall into force immediately.

2. Definitions: In this Act, unless the context otherwise requires,–

1) **"digital signature"** means data in an electronic form, which–

a) is related with any other electronic data directly or logically; and

b) is able to satisfy the following conditions for validating the digital signature–

i) affixing with the signatory uniquely;

ii) capable to identify the signatory;

iii) created in safe manner or using a means under the sole control of the signatory; and

iv) related with the attached data in such a manner that is capable to identify any alteration made in the data thereafter.

2) **"digital signature certificate"** means a certificate issued under section 36;

3) **"electronic"** means electrical, digital, magnetic, wireless, optical, electromagnetic or any technology having equivalent such capability;

4) **"electronic data interchange"** means transferring data from one computer to another computer electronically by following a standard for the purpose of organizing information;

34) **"certification practice and description of procedure"** means certification practice and description of procedure defined by the regulation where practices and procedures are written for issuing Digital Signature Certificate;

35) **"Member"** means a member of cyber appeal tribunal constituted under section 82 of this Act;

36) **"signatory"** means a person providing signature generated through signature generating machine or procedure;

37) **"signature verification machine"** means software or hardware used for verifying signature;

38) **"signature generating machine"** means software or hardware used generating data for creating signature;

39) **"Cyber Tribunal" or "Tribunal"** means a cyber tribunal constituted under section 82 of this Act;

40) **"Cyber Appeal Tribunal"** means a cyber appeal tribunal constituted under section 82 of this Act.

3. Overriding effect of the Act: Notwithstanding anything contained to the contrary in any other law for the time being in force, the provisions of this Act shall have effect.

4. Inter-state application of the Act: 1) If any person commits offence or contravention under this Act outside of Bangladesh which is punishable under this Act if he commits it in Bangladesh, then this Act shall apply as such he commits offence or contravention in Bangladesh.

2) If any person commits offence or contravention in Bangladesh under this Act from outside Bangladesh using a computer, computer system or computer network located in Bangladesh, then this Act shall apply as such the entire process of the offence or contravention took place in Bangladesh;

3) If any person from within Bangladesh commits offence or contravention outside of Bangladesh under this Act, then this Act shall apply against him as such the entire process of the offence or contravention took place in Bangladesh;

Chapter–2
Digital Signature and Electronic Records

5. Authentication of electronic records by digital signature: 1) Subject to the provision of sub-section (2) of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

2) The authentication of electronic record shall be effected by the use of technology neutral system or standard authentic signature generating

6. Legal recognition of electronic records: Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such information or matter is rendered or made available in an electronic form:

Provided that such information or matter is accessible so as to be usable for a subsequent reference.

7. Legal recognition of digital signatures: Where any law provides that–

a) any information or any other matter shall be authenticated by affixing the signature; or

b) any document shall be authenticated by signature or bear the signature of any person;

then, notwithstanding anything contained in such law, such information or matter is authenticated by meathe case of any document.

8. Use of electronic records and electronic signatures in Government and its agencies: 1) Where any law provides for–

a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

b) the issue or grant of any licence, permit, sanction, approval or order by whatever name called in a particular manner;

c) the receipt or payment of money in a particular manner;

then, notwithstanding anything contained in such law, filing, issue, grant of the document and receipt and payment of money, as the case may be, is effected by means of prescribed electronic form.

2) The manner and format in which such electronic records shall be filed, created or issued and the manner or methods of payment of any fee or charges for creation and filing shall be fixed by the rules for fulfilling the purposes of this section.

9. Retention of electronic records: 1) Where any law provides that any document, record or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied–

a) the information contained therein remains accessible so as to be usable for a subsequent reference;

b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be

c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained:

Provided that this sub-clause does not apply to any information which is automatically generated solely for the purpose of enabling and electronic record to be dispatched or received.

2) A person may satisfy the requirements referred to in sub-section (1) of this section by using the services of any other person, if the conditions in clauses (a) to (c) of that sub-section are complied with.

3) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information.

10. **Electronic gazette:** Where any law requires that any law, rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

11. No liability on Government to accept documents in electronic form: Nothing contained in this Act shall by itself compel any Ministry or Department of the Government or any authority or body established by or under any law or controlled or funded by the Government to accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

12. Power of Government to make rules in respect of digital signatures: The Government may, by notification in the Official Gazette and in additionally optionally in the Electronic Gazette,make the following rules (all or any of them) to prescribe for the purposes of this Act–

a) the type of digital signature;

b) the manner and format in which the digital signature shall be affixed;

c) the manner and procedure which facilitates identification of the person affixing the digital signature;

d) the control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records and payments; and

e) any other matter which is necessary to give legal effect to digital signatures.

15. Time and place of dispatch and receipt of electronic record: 1) Save as otherwise agreed to between the originator and the addressee–

a) the time of dispatch of an electronic record shall be determined when it enters a computer or electronic machine or resource out side the control of the originator;

b) the time of receipt of an electronic record shall be determined as follows, namely:--

i) if the addressee has designated an electronic device or resource for the purpose of receiving electronic records, receipt occurs,–

a) at the time when the electronic record enters the designated electronic device or resource;

b) if the electronic record is sent to an electronic device or resource of the addressee that is not designated electronic device or resource, at the time when the electronic record is retrieved by addressee;

ii) if the addressee has not designated an electronic device or resource along with the specified timings, if any, receipt occurs when the electronic record enters the electronic device or resource.

c) an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

2) The provision of sub-section (1) (b) of this section shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (1) (c) of this section.

3) For the purposes of this section,–

a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

Explanation: "principal place of business" or **"usual place of residence"** in relation to a body corporate or body incorporated means the place where it is registered.

Chapter–4
Secure Electronic Records & Digital Signatures

16. Secure electronic record: Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to a secure electronic record from such point of time to the time of verification.

after exercising reasonable care or using any agreed procedure, that the transmission resulted in any error in the electronic record as received.

7) The addressee shall be entitled to regard each electronic record received as separate electronic record and to act on that assumption; however, it shall not be applicable for the following electronic records–

a) duplicates of other electronic records created by the addressee; and
b) the addressee knew or should have known, after exercising reasonable care or using any agreed procedure, that the electronic record was a duplicate.

14. Acknowledgement of receipt.—1) Sub-sections (2), (3) & (4) of this section shall apply where, on or before sending an electronic record, or by means of that electronic record, the riginator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.

2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by–

a) any communication by the addressee, automated or otherwise; or
b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

3) Where the originator has stipulated that the electronic record shall be conditional on receipt of the acknowledgement, then, until the acknowledgement has been received, the electronic cord shall be deemed to have been never sent by the originator.

4) Where the originator has not stipulated that the electronic record shall be conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the riginator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time,the originator–

a) may give notice to the addressee stating that no acknowledge-ment has been received and specifying a reasonable time by which the acknowledgement must be received;and
b) if no acknowledgement is received within the time specified in clause (a) of this sub- section, may, after giving notice to the addressee, treat the electronic record as though it has never been sent.

5) Where the originator receives the addressee's acknowle-dgement of receipt, it shall be presumed that the related electronic record was received by the addressee, but that presumption shall not imply that the content of the electronic record corresponds to the content of the record received.

6) Where the received acknowledgement states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it shall be presumed that those requirements have been met.

Chapter–3
Attribution, Acknowledgment and Despatch of Electronic Records

13. Attribution: 1) An electronic record shall be that of the originator it was sent by the originator himself.

2) As between the originator and the addressee, an electronic record shall be deemed to be that of the originator if it was sent –

a) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

b) by an information system programmed by or on behalf of the originator to operate automatically.

3) As between the originator and the addressee, an addressee shall be entitled to regard an electronic record as being that of the originator and to act on that assumption if–

a) in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

b) the information as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify the electronic records as its own.

4) Sub-section (3) of this section shall not apply–

a) from the time when the addressee has received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;

b) in such case as in clause (b) of section (3) of this section, at any time when the addressee knew or ought to have known, after using reasonable care or using agreed procedure, that the electronic record was not that of the originator;

c) if, in all circumstances of the case, it is unconscionable for the addressee to regard the electronic record as being that of the originator or to act on that assumption.

5) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee shall be entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption.

6) Whatever is there in sub-section (5) of this section, the addressee shall not be so entitled when the addressee knew or should have known,

17. Secure digital signature: 1) If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was–

a) unique to the person affixing it;

b) capable of identifying the person affixing it; and

c) created in manner or using a means under the sole control of the person affixing; then such digital signature shall be deemed to be a secure digital signature as per sub-section (2).

2) Despite the fact of sub-section (1), the digital signature would be invalidated if the electronic record was altered relating to this very digital signature.

Chapter–5
Contoller & Other Officers, etc.

18. Controller and other officers etc: 1) For the purpose of this Act, the Government may, by notification in the Official Gazette and additionally optionally in Electronic Gazette, appoint a Controller and such number of Deputy Controller(s) and Assistant ontroller(s) as it deems fit:

Provided that, the period will not be more then one year from the dates of notification.

2) The Controller shall discharge such functions as are vested in him under this Act under the general superintendence and control of the Government.

3) The Deputy Controllers and the Assistant Controllers shall perform such functions as are assigned to them by the Controller under the general superintendence and control of the Controller.

4) The qualifications, experience and terms & conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Service Code.

5) The Head Office of the Controller shall be located at Dhaka and as the Government may think fit may establish Branch Offices at such places for fixed time duration or permanently.

6) There shall be a seal of the office of the controller, which will be used in places approved by the Government and other defined areas.

7) For the purpose of preserving all electronic records under this Act there shall be a room in the Office of Controller which will be named as "electronic records repository room."

19. Functions of the Controller: The Controller may perform all or any of the following functions, namely.–

a) exercising supervision over the activities of the Certifying Authorities;

b) laying down the standards to be maintained by the Certifying Authorities;
c) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
d) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
e) specifying the contents of written, printed or visual materials and advertisements that may be used in respect of a Digital Signature Certifying;
f) specifying the form and content of a Digital Signature Certificate;
g) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
h) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them for auditing the Certifying Authorities;
i) facilitatining the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
j) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
k) resolving any conflict of interests between the Certifying Authorities and the subscribers;
l) laying down the duties and responsibilities of the Certifying Authorities;
m) maintaining computer based databases, which--
   i) contain the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations; and
   ii) shall be accessible to the member of the public;
n) perform any other function under this Act or Codes prepared under this Act.

20. Recognition of foreign Certifying Authorities: 1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may, with the previous approval of the Government, and by notification in the Official Gazette and additionally optionally in Electronic Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

2) Where any Certifying Authority is recognized under sub-section (1) of this section, the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it

was granted recognition under sub-section (1) of this section, for reasons to be recorded in writing, by notification in the Official Gazette and additionally optionally in Electronic Gazette, revoke such recognition.

21. Controller to act as repository: 1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

2) The Controller shall ensure that the secrecy and security of the digital signature are assured and in order to do so shall make use of hardware, software and procedures that are secure from intrusion and misuse and follow such standards as may be prescribed.

22. Licence to issue Digital Signature Certificate: 1) Subject to the provision of sub-section (2) of this section, any person may make an application to the Controller for a licence to issue Digital Signature Certificates.

2) No licences shall be issued under sub-section (1) of this section unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities which are necessary to issue Digital Signature Certificates.

3) A licence granted under sub-section (1) of this section–

a) shall be valid for certain period;

b) shall be delivered subject to fulfilling defined terms and conditions; and

c) shall not be transferable or heritable.

23. Application for licence: 1) Every application for issue of a licence shall be submitted in a prescribed form.

2) Every application of sub-section (1) of this section shall be accompanied by–

a) a certification practice statement;

b) necessary documents with respect to identification of the applicant

34. Surrender of licence: Every Certifying Authority whose licence is revoked or suspended, as the case may be, shall immediately after such revocation or suspension, as the case may be, surrender the licence to the Controller.

35. Disclosures: 1) Every Certifying Authority shall disclose in the manner specified by regulations–

a) digital signature certificate used by the Certifying Authority to digitally sign another Digital Signature Certificate;
b) any certification practice statement relevant thereto;
c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and
d) any other fact the materially and adversely affects either the reliability of a Digital Signature Certificate, which the Certifying Authority has issued, or the Certifying Authority's ability to perform its service.

2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then the Certifying Authority shall use reasonable efforts to notify any person who is likely to affected by the occurrence, or act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

36. Issue of certificate: The Certifying Authority may issue a certificate to a prospective subscriber only after the Certifying Authority–

a) has received an application in the prescribed form requesting for issuance of a certificate from the prospective subscriber;
b) if it has a certification practice statement, complied with all of the practices and procedures set forth in such certification practice
c) if the prospective subscriber is the person to be listed in the certificate to be issued;
d) if all information in the certificate to be issued is correct; and
e) whether the prospective subscriber paid such fees as may be prescribed for issuance of certificate.

37. Representations upon issuance of certificate: 1) By issuing a certificate, the Certifying Authority represents to any person who reasonably relies on the certificate or digital signature described in the certificate that the Certifying Authority has issued the certificate in accordance with any applicable certification practice statement [illegible]

are vested in a Civil Court under the Code of Civil Procedure, when trying a suit in respect of the following matters, namely:–

a) discovery and inspection;

b) enforcing the attendance of any person and examining him on oath or affirmation;

c) compelling the production of any document; and

d) issuing commissions for the examination of witness.

30. Access to computers and data: 1) Without prejudice to the provisions of section 45 of this Act the Controller or any officer authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act or rules and regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

2) For the purpose of sub-section (1) of this section the Controller or any officer authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

3) If authorization has been given to a person, the authorized person shall oblige to assist as instructed under sub-section (1) of this section.

31. Certifying Authority to follow certain procedures: Every Certifying Authority shall–

a) make use of hardware, software and procedures that are secure from intrusion and misuse;

b) provide a reasonable level of reliability in its services which are reasonable suited to the performance of intended function under this Act;

c) adhere to security procedures to ensure that the secrecy and privacy of digital signatures are assured; and

d) observe such other standards as may be specified by regulations.

32. Certifying Authority to ensure compliance of the Act, rules regulations, etc: Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations or orders made thereunder.

33. Display of licence: Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

a) made statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

b) failed to comply with the terms and conditions subject to which the licence was granted;

c) failed to main the standards specified under section 21(2) of this Act;

d) contravened any provisions of this Act, rules, regulations or orders made thereunder.

2) No licence shall be revoked unless the Certifying Authority has been given reasonable opportunity of showing cause against the proposed revocation under sub-section (1) of this section.

3) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1) of this section, by or, suspend such licence temporarily pending the completion of any enquiry ordered by him.

4) No licence shall be suspended for a period exceeding 14 (fourteen) days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the propose suspension under sub-section (3) of this section;

5) A Certifying Authority whose licence has been suspended temporarily shall not issue any Digital Signature Certificate during the period of such suspension.

27. Notice of revocation or suspension of licence: 1) Where the licence of a Certifying Authority is revoked or suspended temporarily, the Controller shall publish notice of such revocation or suspension, as the case may be, in the database maintained by him.

2) Where one or more repositories are specified, the Controller shall publish notices of such temporarily revocation or suspension, as the case may be, in all such repositories:

Provided that the database containing the temporarily notice of such revocation or suspension, as the case may be, shall be made available electronically including website or any other medium which shall be accessible round the clock.

28. Power to delegate: The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any other officer to exercise any of the power of the Controller under this Act.

29. Power to investigate contraventions: 1) The Controller or any officer authorized by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

2) The Controller or any officer authorized by him in this behalf shall, for the purposes of sub-section (1) of this section, have the same power as

a) the Certifying Authority has complied with all applicable requirements of this Act and the rule and regulations made thereunder in issuing the certificate, and if the Certifying Authority has published the certificate or otherwise made it available to such relying person, that the subscriber listed in the certificate has accepted it;

b) all information in the certificate is accurate, unless the Certifying Authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed;

c) the Certifying Authority has no knowledge of any material fact which if it had been included in the certificate would adversely effect the reliability of the representations in clauses (a) and (b) of this sub-section.

3) Where there is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person has notice, sub-section (2) of this section shall apply to the extent that the representations are not inconsistent with the certification practice statement.

38. Revocation of Digital Signature Certificate: A Certifying Authority shall revoke a Digital Signature Certificate issued by it–

a) where the subscriber or any person authorized by him makes a request to that effect; or

b) upon the death of the subscriber; or

c) where the subscriber is a firm or a company, if it has been dissolved or wound up or has otherwise ceased to exist.

2) Subject to the provisions of sub-section (3) of this section and without prejudice to the provisions of sub-section (1) of this section, a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time if it is of opinion that–

a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

c) the Certifying Authority's identification/security system was compromised in a manner materially or as a whole affecting the Digital Signature Certificate's reliability;

d) the subscriber has been declared insolvent by a competent court or authority.

3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Suspension of Digital Signature Certificate: 1) Subject to the provisions of sub-section (2) of this section, the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate–

a) on receipt of a request to that effect from the subscriber listed in the Digital Signature certificate or any person duly authorized to act on behalf of that subscriber;

b) if it is opinion that the Digital Signature Certificate should be suspended in public interest.

2) A Digital Signature Certificate shall not be suspended for a period exceeding 30 (thirty) days without giving the subscriber a notice under sub-section 1 (b) of this section.

3) Certifying Authority can suspend the Digital Signature Certificate, if the Authority is satisfied on the ground that the explanation given by the subscriber in response to the notice of sub- ection (2) of this section is not acceptable.

4) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

40. Notice of revocation or suspension: 1) Where a Digital Signature Certificate is revoked under section 38 of this Act or suspended under section 39 of this Act, the Certifying Authority shall publish a notice of such revocation or suspension, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such revocation or suspension, as the case may be, in all such repositories.

Chapter–6
Duties of Subscribers

41. Application of security procedure: The subscriber shall apply required security procedure to ensure the purity of Digital Signature Certificate issued by a Certifying Authority.

42. Acceptance of Digital Signature Certificate: 1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate to one or more persons or in a repository.

2) By accepting Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that–

a) all representations made by the subscriber to the Certifying [illegible] relevant to the information contained in

b) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

43. Presumption of represented information of obtaining Digital Signature Certificate: All material representations made by the subscriber to a Certifying Authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in the Digital Signature Certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the Certifying Authority.

44. Control of safety measure of subscriber: 1) Every subscriber shall exercise reasonable care to retain control of using of Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.

2) If the security of Digital Signature Certificate has been compromised by disobeying the rules in sub-section (1) of this section, the subscriber shall communicate the same without any delay to the Certifying Authority who has issued the Digital Signature Certificate in an agreed manner.

Chapter–7
Penalites and Adjudication, Etc.

45. Power of Controller to give directions: The Controller may, by order, direct a Certifying Authority or any employee of such a Certifying Authority to take such measure or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, or rules and regulations made thereunder.

46. Power of Controller to give directions in emergency: 1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty, integrity, or security of Bangladesh, friendly relations of Bangladesh with other States, public order or for preventing incitement to commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information to be transmitted through any computer resource.

2) The subscriber or any person in charge of a computer resource shall, when called upon by any agency to which direction has been issued under sub-section (1) of this section, extend all facilities and technical assistance to decrypt the information.

47. Power to announce protected systems: 1) The Controller may, by notification in the Official Gazette or in Electronic Gazette, declare any computer, computer system or computer network to be a protected system.

2) The Controller, by order in writing, authorize the persons who are authorized

g) provides any assistance to any person to facilitate access to a computer, computer system or computer network, in contravention of the provisions of this Act, rules or regulations made thereunder;

h) for the purpose of advertisement of goods and services, generates or causes generation of spams or sends unwanted electronic mails without any permission of the originator or subscriber;

i)charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network; then the above said activities shall be treated as offences of the said person.

2) If any person commits offence under sub-section (1) of this section, he shall be punishable with rigorous imprisonment for a term which may extend to fourteen years and minimum seven years, or fine upto 10 lacs Taka or for the both of the above..

Explanation: For the purpose of this section–

i) **"computer contaminant"** means any set of computer instructions that are designed--

a) to modify, destroy record, transmit data or program residing within a computer, computer system or computer network; or

b) by any means to usurp the normal operation of the computer, computer system or computer network;

ii) **"computer database"** means a representation information, knowledge, facts, concepts or instructions in the form of text, image, audio or video that--

a) are being prepared or have been prepared in a formalized manner by a computer, computer system or computer network; and

b) are intended for use in a computer, computer system or computer network;

iii) **"computer virus"** means such computer instruction, information, data or program, that--

a) destroys, damages, degrades or adversely affects the performance of a computer resource; or

b) attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer;

iv) **"damage"** means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

55. Punishment for tampering with computer source code: 1) Whoever intentionally or knowingly conceals, destroys or alters or intentionally or knowingly causes other person to conceal, destroy or alter any computer

3) If any instruction under sub-sections (1) and (2) of this section is given to anyone, he shall be bound to obey it.

4) If any person breaches the given instructions of this section, the Controller can fine the person which may extend to Taka ten thousand.

53. Penalties: 1) The Controller can impose penalties for breaching other rules under this Act defined by the rules as an addition to imposable penalties under this Act.

2) No penalty shall be imposed under this Act for breaching this Act or any rules of this Act without giving reasonable opportunity to the offender on hearing.

3) The accused person can lodge an application to the Controller for auditing the decision of imposing penalties by the Controller within seven days from the date the decision is made and if any such application is lodged, the Controller shall give opportunity to the Applicant for hearing and dissolve it within fifteen days.

4) Unless the penalties are paid under this Act which is due, is collectable as a Government demand under the Public Demands Recovery Act, 1913 (Ben. Act III of 1913).

Chapter–8
Offences, investigation, adjudication, penalties, Etc.

Part –I: Crime and Punishment

54. Penalty for damage to computer, computer system, etc: 1) If any person, without permission of the owner or any person who is in charge of a computer, computer system or computer network,–

a) accesses or secure access to such computer, computer system or computer networks for the purpose of destroying information or retrieving or collecting information or assists other to do so;

b) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

d) damages or causes to be damaged willingly in any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

e) disrupts or causes disruption of any computer, computer system or computer network;

f) denies of causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

48. Penalty for failure to furnish document, return and report: If any person fails to submit given document, return and report under the provisions of this Act, or rules and regulations made thereunder to the Controller or Certifying Authority, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person which may extend to Taka ten thousands mentioning reasons in written by administrative order.

49. Penalty for failure to file return, information, book etc: If any person fails to deliver any information, books or any other documents under the provisions of this Act, or rules and regulations made thereunder within stipulated time, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person which may extend to Taka ten thousand mentioning reasons in written by administrative order.

50. Penalty for failure to maintain books of accounts or record: If any person fails to maintain books of accounts or records which is supposed to be preserved under the provisions of this Act, or rules and regulations made thereunder, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person which may extend to Taka two lakhs mentioning reasons in written by administrative order.

51. Residuary penalty: If any person contravenes any rules of this Act for which the provision of penalties has not been fixed separately under the provisions of this Act, or rules and regulations made thereunder, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person for breaching the very rule which may extend to Taka twenty five thousands mentioning reasons in written by administrative order.

52. Power of Controller to issue prohibition of possible breaching of rules: 1) If the Controller is in the opinion that, any person has attempted or is attempting to do such activities which is breaching or may breach the provisions of this Act, rules, regulations made thereunder, or conditions or any order of the Controller then the Controller shall issue a notice within the stipulated time limit ordering the person to present his statement in written why he should not refrain himself from doing such activity and if such statement is presented then the Controller shall issue an order to refrain him from doing such activity or any other instruction about the activity sthat deems fit to him.

2) If the Controller is satisfied that, the nature of breaching or possible breaching under sub-section (1) of this section is such that to prevent the person from that activity immediately, then the Controller shall issue an interim order [illegible] notice under that sub-section.

source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by any law for time being in force, then this activity of his will be regarded as offence.

2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to three years, or with fine which may extend to Taka three lakhs, or with both.

Explanation: For the purpose of this section, "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resources in any form.

56. Punishment for hacking with computer system: 1) 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 and thereby destr-oys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

b) damage through illegal access to any such computer, computer network or any other electronic system which do not belong to him;then such activity shall be treated as hacking offence.

2) Whoever commits hacking offence under sub-section (1) of this section he shall be punishable with rigorous imprisonment for a term which may extend to maximum 14 years and minimum 7 years, or with fine which may extend to Taka one crore, or with both.

57. Punishment for publishing fake, obscene or defaming information in electronic form: 1) If any person deliberately publishes or transmits or causes to be published or transmitted in the website or in electronic form any material which is fake and obscene or its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence.

2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to maximum 14 years and minimum 7 years and with fine which may extend to Taka one crore.

58. Punishment for failure to surrender licence: 1) Where any Certifying Authority fails to surrender a licence under section 34 of this Act, the person in whose favour the licence is issued, the failure of the person shall be an offence.

2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to six months, or with fine which may extend to Taka ten thousands, or with both.

59. Punishment for failure to comply with order: 1) Any person who fails to comply with any order made under section 45 of this Act, then this activity of his will be regarded as an offence.

2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to one year, or with fine which may extend to Taka one lakh, or with both.

60. Punishment for failure to comply with order made by the Controller in emergency: 1) Any person who fails to comply with any order made under section 46 of this Act, then this activity of his will be regarded as an offence.

2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to five years, or with fine which may extend to Taka five lakhs, or with both.

61. Punishment for unauthorized access to protected systems: 1) Any person who secures access or attempts to secure access to protected system in contraventions of section 47 of this Act, then this activity of his will be regarded as an offence.

2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to maximum 14 years and Minimum 7 years, or with fine which may extend to Taka ten lakhs, or with both.

62. Punishment for misrepresentation and obscuring information: Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate shall be regarded as an offence.

2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

63. Punishment for disclosure of confidentiality and privacy: 1) Save as otherwise provided by this Act or any other law for the time being in force, no person who, in pursuance of any of the owers conferred under this Act, or rules and regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register, correspondence, information, document or other material to any other person shall be regarded as an offence.

2) Whoever commits any offence under sub-section (1) of this

64. Punishment for publishing false Digital Signature Certificate: No person shall publish a Digital Signature Certificate or otherwise make it available to any other person knowing that–

a) the Certifying Authority listed in the certificate has not issued it; or

b) the subscriber listed in the certificate has not accepted it; or

c) the certificate has been revoked or suspended;

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation and by breaching the rules such Digital Signature Certificate is ublished or otherwise make it available to others shall be regarded as an offence.

2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

65. Punishment for publishing Digital Signature Certificate for fraudulent purpose etc: Whosoever knowingly creates and publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be regarded as an offence.

2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakh, or with both.

66. Punishment for using computer for committing an offence: 1) Whosoever knowingly assists committing crimes under this Act, using any computer, e-mail or computer network, resource or system shall be regarded as an offence.

2) Whoever aids committing any offence under sub-section (1) of this section he shall be punishable with the punishment provided for the core offence.

67. Offences committed by companies etc: If any offence is committed by a company under this Act, then each director, manager, secretary, partner, officer and staff of the company who has directly involvement in committing the said offence shall be guilty of the offence or the contraventions, as the case may be, unless he proves that the offence or contravention was committed without his knowledge or that he exercised sue diligence in order to prevent commission of such offence or contravention.

Explanation: For the purposes of this section –

a) **"company"** means any body corporate and includes commercial firm, partnership business, cooperatives, association, organization or other association of individuals; and

b) **"director"** in relation to a commercial firm includes a partner or member of Board of Directors.

the Tribunal can order the accused person to appear before the Tribunal by publishing such order in two mass circulated national Bengali dailies and if the accused person fails to do so, the prosecution shall take place in his absence.

5) The rules mentioned in sub-section (4) of this section shall not be applicable if the accused person fails to appear before the Tribunal or absconded after getting bail.

6) The Tribunal can order any police officer, or the Controller, or any officer authorized by the Controller, as the case may be, to reinvestigate the case and submit the report within the stipulated time of its own initiative or any application lodged to the Tribunal,

70. Application of Code of Criminal Procedure in the activities of Tribunal: 1) Rules of Code of Criminal Procedure, as far as, are not inconsistent with the rules of this Act shall be applicable in the activities of this Tribunal and it will have all the power as exercised by the Session Court.

2) The person prosecuting the case on behalf of the Government in this tribunal to be known as public prosecutor.

71. Rules relating to bail: The Judge of Cyber Tribunal shall not bail any person accused in committing crime under this Act, which is punishable, unless–

a) Hearing opportunity is given to the Government side on similar bail orders;

b) The Judge is satisfied that,–.

i) There is reasonable cause to believe that the accused person may not be proved guilty in the trial;

ii) The offence is not severe in relative term and the punishment shall not be tough enough even the guilt is proved.

c) He writes down the reasons of similar satisfactions.

72. Time limit to deliver verdict: 1) The Judge of Cyber Tribunal shall give the verdict within ten days from the date of completing of taking evidence or debate, what happened later, unless he extends the time limit no more than ten days with having written reasons.

2) If the verdict is given by the Cyber Tribunal under sub-section (1) of this section or any appeal is lodged against the verdict to the Cyber Appellate Tribunal then Cyber Tribunal or Cyber Appellate Tribunal concerned shall forward the copy of the verdict of the appeal to the Controller for preserving it in the electronic records repository room established under section 18 (7) of this Act.

73. Prescribed timeframe for dissolving cases by Cyber Tribunal: 1) The Judge of Cyber Tribunal shall complete the prosecution within six months since the date of filing the charge sheet.

Part–II: Establishment of Cyber Tribunal, Investigation of Offences, Adjudication, Appeal Etc.

68. Establishment of Cyber Tribunal: 1) The Government shall, by notification in the Official Gazette, establish one or more Cyber Tribunals to be known as Tribunal at times for the purposes of speedy and effective trials of offences committed under this Act.

2) Cyber Tribunal established under sub-section (1) of this section in consultation with the Supreme Court shall be constituted by a Session Judge or an Additional Session Judge appointed by the Government; and similarly appointed a Judge to be known as "Judge, Cyber Tribunal."

3) Local jurisdiction of entire Bangladesh or jurisdiction of one or more Session Divisions can be given to the Cyber Tribunal established under this Act; and the Tribunal only prosecutes the offences committed under this Act.

4) The on-going prosecution of any case of any Session Court shall not be suspended or transferred automatically to the Tribunal of local jurisdiction concerned due to tendering of local jurisdiction of entire Bangladesh or parts of jurisdiction constituted by one or more Session Divisions to the Tribunal established by the Government later on, however, the Government by notification in the Official Gazette, transfer the case to the Tribunal having special local jurisdiction.

5) Any Tribunal, taken decision otherwise, shall not be bound to retaking statement of witness who has already given statement, or taking rehearing or begin again any other activities already undertaken under sub-section (1) of this section, however, the Tribunal shall continue the prosecution from where it stood on the basis of already taken or presented statement from the witness.

6) The Government, by order, shall define the place and time; accordingly the special Tribunal shall conduct its activities from that place and time.

69. Trial procedure of Cyber Tribunal: 1) Without written report of a police officer not below the rank of Sub-Inspector or the prior approval of the Controller or any other officer authorized by the Controller the special Tribunal shall not accept any offence trial.

2) The Tribunal shall follow the rules mentioned in the Chapter 23 of the Code of Criminal Procedure, if they are not inconsistent with the rules of this Act, which is used in Session Court.

3) Any Tribunal shall not suspend any prosecution without having written reasons and unless it is required for the sake of just adjudication.

4) If the Tribunal is in the opinion that the accused person has been absconded and for that it is not possible to arrest him and produce him before the Tribunal and there is no possibility to arrest him immediately, in that case

Part–II: Establishment of Cyber Tribunal, Investigation of Offences, Adjudication, Appeal Etc.

68. Establishment of Cyber Tribunal: 1) The Government shall, by notification in the Official Gazette, establish one or more Cyber Tribunals to be known as Tribunal at times for the purposes of speedy and effective trials of offences committed under this Act.

2) Cyber Tribunal established under sub-section (1) of this section in consultation with the Supreme Court shall be constituted by a Session Judge or an Additional Session Judge appointed by the Government; and similarly appointed a Judge to be known as "Judge, Cyber Tribunal."

3) Local jurisdiction of entire Bangladesh or jurisdiction of one or more Session Divisions can be given to the Cyber Tribunal established under this Act; and the Tribunal only prosecutes the offences committed under this Act.

4) The on-going prosecution of any case of any Session Court shall not be suspended or transferred automatically to the Tribunal of local jurisdiction concerned due to tendering of local jurisdiction of entire Bangladesh or parts of jurisdiction constituted by one or more Session Divisions to the Tribunal established by the Government later on, however, the Government by notification in the Official Gazette, transfer the case to the Tribunal having special local jurisdiction.

5) Any Tribunal, taken decision otherwise, shall not be bound to retaking statement of witness who has already given statement, or taking rehearing or begin again any other activities already undertaken under sub-section (1) of this section, however, the Tribunal shall continue the prosecution from where it stood on the basis of already taken or presented statement from the witness.

6) The Government, by order, shall define the place and time; accordingly the special Tribunal shall conduct its activities from that place and time.

69. Trial procedure of Cyber Tribunal: 1) Without written report of a police officer not below the rank of Sub-Inspector or the prior approval of the Controller or any other officer authorized by the Controller the special Tribunal shall not accept any offence trial.

2) The Tribunal shall follow the rules mentioned in the Chapter 23 of the Code of Criminal Procedure, if they are not inconsistent with the rules of this Act, which is used in Session Court.

3) Any Tribunal shall not suspend any prosecution without having written reasons and unless it is required for the sake of just adjudication.

4) If the Tribunal is in the opinion that the accused person has been absconded and for that it is not possible to arrest him and produce him before the Tribunal and there is no possibility to arrest him immediately, in that case

2) If the Judge of Cyber Tribunal fails to complete the prosecution within the time limit fixed under sub-section (1) of this section can extend the time limit another three months having written the reasons.

3) If the Judge of Cyber Tribunal fails to complete the prosecution within the timeframe fixed under sub-section (2) of this section can continue the prosecution process having written the reasons and submitted it as a report to the High Court and the Controller.

74. Prosecution of offence by Session Court: Whatever is contained in the Code of Criminal Procedure, until the special tribunal has not been established, the Session Court shall prosecute any offence committed under this Act.

75. Prosecution procedure followed by the Session Court: 1) To prosecute any offence committed under this Act which is trialed in Session Court, Session Court shall follow the rules mentioned in section 23 of the Code of Criminal Procedure which is applicable in Session Court trial.

2) Any Session Court shall not accept any prosecution/trial of any offence committed under this Act without any written report from the police officer not below the rank of Sub-Inspector of the Police and prior approval of the Controller or any officer authorized by the Controller, whatever is contained in the Code of Criminal Procedure.

76. Investigation of crime, etc: 1) Whatever is contained in the Code of Criminal Procedure, the Controller or any officer authorized by the Controller, or any police officer not below the rank of Sub-Inspector of the Police shall investigate any offence committed under this Act.

1A) Whatever is contained in sub-section (1) of section 76 of this Act, Collector or any other official having authority from the Collector or any Police Officer under this sub-section shall not investigate any offence committed under this Act.

1B) At any step of the investigation of a cases, from the collector for logical investigation, investigation coduct –

a) Collector or official having authority from the collector empowered by the Police Officer; or

b) Police Officer authorizes by the Collectoir or official having authority from the collector,

where shift is essential, the Government in that case by order from Cyber Tribunal, transfer, cases from Collector or official having authority from Collector to the Police Officer, or Police officer to Collector or

a) Sections 54, 56, 57 & 61's offence shall be cognizable and non-bailable; and

b) Sections 55, 58, 59, 60, 62, 63, 64 & 65 's offence shall be non-cognizable and bailable.

77. **Confiscation:** 1) Any computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, or in respect of which any offence has been committed, shall be liable to confiscation by an order of the court trying an offence or contravention.

2) If the court is satisfied, that the computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories belonging to a person or under control of him related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has not been responsible to contravene, or committing an offence, then the computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories shall not be confiscated.

3) If any legal computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories is found with the computer, computer system, floppies, compact disks (CDs),tape drives or any other accessories which is confiscated under sub-section (1) of this section shall also be confiscated.

4) Any computer or other relevant accessories belonging to the Government or Body Government Authority is used to commit an offence under sub-section (1) of this section, whatever contained in this section, shall not be confiscated.

78. Penalties or confiscation no bar against other punishments: No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby may be liable under any other law for the time being in force.

79. Network service providers not to be liable in certain cases: For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, or rules and regulations made thereunder, for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised due diligence to prevent the commission of such offence or contravention.

Explanation: For the purposes of this section,–

a) **"network service provider"** means an intermediary;

b) **"third party information"** means any information dealt with by a network service provider in his capacity as an intermediary.

80. Power of seize or arrest: Any investigation taken under this Act, the Controller, or any officer of Government authorized by the Government or any police officer not below the rank of a Sub-Inspector of Police are in opinion that an offence has been committed or being committed or offence which is punishable under this Act has been committed, then having written the reasons, may enter the place and search and seize the germane materials and arrest the concerned person or the offender.

81. Procedure of search, etc: The provisions of the Code of Criminal Procedure shall, subject to the provisions of this Act, apply, so far as may be, in relation to all investigations, entry, search and arrest made under this Act.

Part –III: Estabilsihment of Cyber Appeal Tribunal, etc.

82. Establishment of Cyber Appellate Tribunal: 1) The Government shall, by notification in the Official Gazette, establish one or more Cyber Appellate Tribunals to be known as appellate Tribunal.

2) Cyber tribunal established under sub-section (1) of this section shall consist of one Chairman and two members to be appointed by the Government.

3) A person shall not be qualified as the Chairman of a Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of the Supreme Court and one of the members shall be serving in judicial department or retired District Judge and the other member shall be a person having adequate knowledge and experience in information and communication technology.

4) Chairman and members shall be retained in the positions since the date of joining between no less than three years and no more than five years and their terms of reference shall be determined by the Government.

83. Procedure and powers of Cyber Appellate Tribunal: 1) Cyber Appellate Tribunal shall have the power to hear appeal and dissolving the verdict and order given by Cyber Tribunal and Session Court, as the case may be.

2) In case of hearing and dissolving the appeal, Cyber Appellate Tribunal shall follow the procedure defined by rules and if the rules do not exist in that case Appellate Tribunal shall maintain the procedure in relation to hearing and dissolving of criminal appeal followed by the High Court Division of the Supreme Court.

3) Cyber Appellate Tribunal shall have the power to retain, revoke, alter, or rectify the verdict or order made by the Cyber Tribunal.

4) The decision made by the Appellate Tribunal shall be final.

84. Appeal procedure in case of not establishing Cyber Appellate Tribunal: If the Cyber Appellate Tribunal has not been established, whatever contained in the Code of Criminal rocedure, appeal shall be lodged in the High

4. The Act now allows Government to issue notification on the web thus heralding e-governance.

5. It eases the task of companies of the filing any form, application or document by laying down the guidelines to be submitted at any appropriate office, authority, body or agency owned or controlled by the government. This will help in saving costs, time and manpower for the corporates.

6. The Act also provides statutory remedy to the coporates in case the crime against the accused for breaking into their computer systems or network and damaging and copying the data is proven. The remedy provided by the Act is in the form of monetary damages, not exceeding Tk. 1 crore.

7. Also the law sets up the Territorial Jurisdiction of the Adjudicating Officers for cyber crimes and the Cyber Regulations Appellate Tribunal.

8. The law has also laid guidelines for providing Internet Services on a license on a non-exclusive basis.

1.15. Objections of the ICT Act, 2006:

The preamble of the ICT Act, 2006 declares that an Act to provide legal recognition for transactions 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 alternatives 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[22].

The objectives of the ICT Act-2006 have been illustrated by the Law Commission's Final Report to give effect to the following purposes:[22]

a) to facilitate electronic communications by means of reliable electronic records;

b) 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;

c) to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records;

---

[22] Final Report on the Law of Information Technology, *loc. cit.*, available at http://www.lawcommissionbangladesh.org/wplit.pdf

g) the requirements which an applicant must fulfill;
h) the period of validity of licence;
i) the format in which an application may be made;
j) the amount of fees payable with application for licence;
k) such other document which shall accompany an application for licence;
l) the form of application for renewal of a licence and the fee payable;
m) the form in which application for issue of a Digital Signature Certificate and the amount of fees payable;
n) the qualifications and experience of Chairman and members of Cyber Appeal Tribunal;
o) the form in which appeal may be filed;
p) the procedure of investigation;
q) other such necessary matters.

89. Power of Controller to make regulations: The Controller with prior approval of the Government, by notification in the Official Gazette and in the Electronic Gazette, make for all or any of the following regulations:–

a) the particulars relating to maintenance of database containing the disclosure record of every Certify Authority;
b) the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority;
c) the terms and conditions subject to which a licence may be granted;
d) other standards to be observed by a Certifying Authority;
e) the manner in which the Certifying Authority shall disclose the particular matters;
f) the particulars of statement which shall accompany an application.

90. Original Text & English Text: The original text shall be in Bengali and there shall be a dependable English transcription of it:

Court Division of Supreme Court against the verdict and order given by the Session Court or Cyber Tribunal, as the case may be.

Chapter–9
Miscellaneous

85. Public servants: The Controller, the Deputy Controller, the Assistant Controller or any person empowered under this Act to exercise his power and carrying out the tasks shall be deemed tobe public servants within the meaning of section 21 of Penal Code.

86. Protection of action in good faith: No suit, prosecution or other legal proceedings shall lie against the Government, the Controller, the Deputy Controller, the Assistant Controller or any person acting on his behalf, for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation, order or direction made thereunder.

87. Augmented use of few definitions used in few acts: For the purpose of this Act,–

a) The definition of **"document"** in section 29 of Penal Code, 1860 (Act XLV of 1860) also includes the document generated or prepared by electronic machine or technology;

b) The definition of **"document"** in section 3 of Evidence Act, 1872 (Act I of 1872) also includes the document generated or prepared by electronic machine or technology;

c) The definition of "bankers books" in section 2, Clause (3) of Banker's Books Evidence Act, 1891 (Act XVIII of 1891) also includes the books viz. ledgers, day-books, cash-books, account-books and all other books generated or prepared by electronic machine or technology.

88. Power of Government to make rules: The Government may, by notification in the Official Gazette and in the Electronic Gazette, make for all or any of the following rules for carrying out of this Act:

a) the manner in which any information or matter may be authenticated or any document may be signed by means of digital signature;

b) the electronic form in which filing, issue, grant or payment;

c) the manner and format in which electronic records shall be filed, or issued and the method of payment;

d) the matters relating to the type of digital signature, manner and format in which itmay be affixed;

e) the qualifications, experience and terms and conditions of service of the Controller, Deputy Controllers and Assistant Controllers;

f) other standards to be observed by the Controller;

d) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions.

e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records, and

f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

1.16. What does the ICT Act or Cyber Law enable?

The ICT Act 2006 enables the following matters:

- Legal recognition of Electronic Transaction Record
- Legal recognition of digital signature is at par with the handwritten signature
- Electronic Communication by means of reliable electronic record
- Acceptance of contract expressed by electronic means
- e-Commerce and Electronic Data interchange
- e-Governance
- Electronic filing of documents
- Retention of documents in electronic form
- Uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records or documents
- Publication of official gazette in the electronic form
- Interception of any message transmitted in the electronic or encrypted form
- Prevention of Computer Crime, forged electronic records, international alteration of electronic records fraud, forgery or falsification in e-Commerce and electronic transaction

1.17. Strengths of the Information and Communication Technology Act, 2006

The ICT Act-2006 in Bangladesh is the outcome of the resolution dated 30th January 1997 of the General Assembly of the UNO, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic Commerce on International Trade Law. This resolution recommended, inter alia, that all states give favorable consideration to the said Model Law while

methods of communication and storage of information. The Act is a piece of legislation of its time. The ICT Act-2006 - as yet our lone piece of cyber legislation is a step towards recognizing electronic transactions. The Act has brought radical change in the position of the virtual electronic medium. This Cyber Law will be helpful 'for all aspects of ICT activities including protection of Data Security & Interoperability through Encryption and standards, as well as regulating undesirable text, data and image traffic'[23].

The evaluation of the strengths of the ICT Act under the following issues:

• **Data Theft:** Although there is no definite legal provision that covers data theft, usually the theft of electronic data results in the diminishing of its value. Under such circumstances data theft would be covered under Section 66 of the ICT Act-2006, which recommends a punishment of up to three years imprisonment and / or fine upto Tk. 2lacs or with both. The theft of source or object code is also included under data theft. The specific provision dealing with this is in section 65. A crime under this section is punishable with imprisonment up to three years and / or with fine, which may extend up to Taka twolacs, or with both.

• **Email Abuse:** Sending pornographic or obscene emails are punishable under section 69 of the ICT Act-2006. An offence under this section is punishable on first conviction with imprisonment for a term, which may extend to five years and with fine, which may extend to taka one lakh. In the event of a second or succeeding conviction the optional punishment is imprisonment for a term, which may extend to ten years and also with fine which may extend to taka two lakh.

Data Alteration: Section 56 of the ICT Act-2006 covers unauthorized alteration of data. This section deals with hacking. According to this section – Whoever, with 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 it injuriously by any means, commits the offence of "hacking". Unauthorized alteration of data is punishable under section 68 with three years imprisonment or with fine upto Tk. Two lacs or with both.

• **Unauthorized Access:** Unauthorized access is covered by section 54 of the ICT Act-2006, which affords for a penalty of upto Taka one crore for this offence. According to this section- If any person, without permission of

the owner or any other person who is in charge of a computer, computer system or computer network,

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, or rules and regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network,

he shall be liable to pay to the person affected compensation not exceeding Taka one crore.

• **The Cyber Appellate Tribunal:** The ICT Act-2006 contemplates the constitution of the Cyber Appellate Tribunal under section 82(1) of the Act (Tribunal), having a Presiding Officer under section 83 of the Act. The Tribunal will hear all appeals from orders passed by the Adjudicating Officer. In order to implement the punishments laid down in the ICT Act-2006, the Government will appoint an Adjudicating Officer who will have the powers of a civil court for the purposes of section 195 and Chapter XXXV of the Code of Criminal Procedure-1898 (Act V of 1898) under section 82 of the ICT Act-2006.

• **Bar on Disclosure of Confidentiality and Privacy:** Breach of privacy and confidentiality of electronic record, book, register, correspondence, information, document or other material of a secure nature is rewarded with

with imprisonment for a term which may be 7 years to 14 years and with fine which may extend to one crore Tk. Or with both. It does not specifically talk only cyber defamation. This provision does not cover other crimes, which could have been expressly brought within its sphere such as cyber defamation. Emails or other transmission substances that are defamatory in nature are punishable under Sections 500, 501 and 502 of the Penal Code-1860 which recommends an imprisonment of up to two years or a fine or both after passing the ICT Act-2006.

- Threatening emails or other transmission substances that are defamatory in nature is punishable under the provisions of the Penal Code relevant to criminal intimidation, insult and prejudicial Act under Chapter XXII of the Penal Code.

- **Section 56 of ICT Act Section 23 of the Penal Code:** Section 56 provides provision about hacking as follows:

Whoever, with 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 it injuriously by any means, commits the offence of "hacking".

Section 23 of the Penal Code defines the "wrongful loss" as 'is the loss by unlawful means of property to which the person losing it is legally entitled'.

The law against hacking under section 56 must be applied with minutely and carefully.

Mens-rea and Suit for Damage: In a suit for damage, it is not necessary to prove mens-rea, i.e. intent or knowledge and Actus rea, i.e. the Act of commission, but both of them to be required like all criminal offences to prove in the case of hacking under section 56 of the ICT Act-2006. Since damages can also be claimed by the victims from the hacker and it also is legal to the common criinal law, section 56 of the ICT Act-2006 is not differentiated between civil and criminal suit.

Common Parlance of Section 54 & Section 56 against Contravention: The ICT law declares the provision of penalty for damage to computer, computer system, etc in section 54 as follows:

If any person, without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-

(a) accesses or secures access to such computer, computer system or computer network,

it will not be long before the above provisions are subject to judicial scrutiny and ultimately it would be for the High Courts and the Supreme Court to decide whether the provisions of search, seizure and arrest are arbitrary or not. The coupling between law and technology is socially mediated. Although the newly enacted Cyber Law has some weakness, something is better nothing.

The ICT Law 2006, though appears to be self-sufficient, it takes mixed stand when it comes to many practical situations. It looses its certainty at many places like:

- The law misses out completely the issue of Intellectual Property Rights, and makes no provisions whatsoever for copyrighting, trade marking or patenting of electronic information and data. The law even doesn't talk of the rights and liabilities of domain name holders, the first step of entering into the e-commerce.

- The law even stays silent over the regulation of electronic payments gate way and segregates the negotiable instruments from the applicability of the IT Act, which may have major effect on the growth of e-commerce in Bangladesh. It leads to make the banking and financial sectors irresolute in their stands.

- The Act empowers the Deputy Superintendent of Police to look up into the investigations and filling of charge sheet when any case related to cyber law is called. This approach is likely to result in misuse in the context of Corporate Bangladesh as companies have public offices which would come within the ambit of "public place" under the Act. As a result, companies will not be able to escape potential harassment at the hands of the DSP.

- Internet is a borderless medium; it spreads to every corner of the world where life is possible and hence is the cyber criminal. Then how come is it possible to feel relaxed and secured once this 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?

- The ICT Act is silent on filming anyone's personal Actions in public and then distributing it electronically. It holds ISPs (Internet Service Providers) responsible for third party data and information, unless contravention is committed without their knowledge or unless the ISP has undertaken due diligence to prevent the contravention.

- There is very harsh provision for transmitting any Defamatory Substances by the ICT Act-2006. Though Section 57 of the ICT Act-2006 provides for punishment to whoever transmits or publishes or causes to be published or transmitted any material which is obscene in electronic form

punishment for a term which may extend to two years, a fine which may extend to Tk. one lac, or with both under section 63 of the ICT Act, 2006. And section 63 protects the Constitutional agreement through Art. 43 as follows:

Every citizen shall have the right, subject to any reasonable restrictions imposed by law in the interests of the security of the State, public order, public morality or public health-

(a) to be secured in his home against entry, search and seizure; and

(b) to the privacy of his correspondence and other means of communication.

Section 63 of the Act ensures the privacy from another person as follows:

Save as otherwise provided by this Act or any other law for the time being in force, no person who, in pursuance of any of the powers conferred under this Act, or rules and regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register, correspondence, information, document or other material to any other person.

• **Amendments of other Acts:** The ICT Act-2006 demands amendment of certain Acts for the first step for incorporation of the Internet into Bangladesh's legal framework. There is still a long way to go before the Bangladeshi legal system incorporates and accepts the Internet fully. The Evidence Act-1872, the Bankers' Books Evidence Act-1891 and the Bangladesh Bank Order-1972 shall be amended in the manner specified in the Second Schedule, Third Schedule and Fourth Schedule to this Act.

1.18. Criticism and Weakness of the ICT Act, 2006:

The ICT law has identified some critical situations, which is not clear to our archaic legal provisions. The law does sometimes regulate the social norm and then control of information technology. Ever since the passing of the Information and Communication Technology Act by the Parliament, a lot has been said both for and against the Act. The controversy seems to have largely revolved around the fact that the police have been given unfettered powers to enter and search any place as well as the powers to arrest any person who is reasonably suspected to have committed or is about to commit an offence under the ICT Act. The Government, on its part, has defended the above provisions by arguing that there is nothing new in enacting such a law and that similar provisions already exist in other statutes as well. Besides, there are adequate safeguards in the ICT Act itself, which [illegible] shall apply in

with imprisonment for a term which may be 7 years to 14 years and with fine which may extend to one crore Tk. Or with both. It does not specifically talk only cyber defamation. This provision does not cover other crimes, which could have been expressly brought within its sphere such as cyber defamation. Emails or other transmission substances that are defamatory in nature are punishable under Sections 500, 501 and 502 of the Penal Code-1860 which recommends an imprisonment of up to two years or a fine or both after passing the ICT Act-2006.

- Threatening emails or other transmission substances that are defamatory in nature is punishable under the provisions of the Penal Code relevant to criminal intimidation, insult and prejudicial Act under Chapter XXII of the Penal Code.

- **Section 56 of ICT Act Section 23 of the Penal Code:** Section 56 provides provision about hacking as follows:

Whoever, with 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 it injuriously by any means, commits the offence of "hacking".

Section 23 of the Penal Code defines the "wrongful loss" as 'is the loss by unlawful means of property to which the person losing it is legally entitled'.

The law against hacking under section 56 must be applied with minutely and carefully.

Mens-rea and Suit for Damage: In a suit for damage, it is not necessary to prove mens-rea, i.e. intent or knowledge and Actus rea, i.e. the Act of commission, but both of them to be required like all criminal offences to prove in the case of hacking under section 56 of the ICT Act-2006. Since damages can also be claimed by the victims from the hacker and it also is legal to the common criinal law, section 56 of the ICT Act-2006 is not differentiated between civil and criminal suit.

Common Parlance of Section 54 & Section 56 against Contravention: The ICT law declares the provision of penalty for damage to computer, computer system, etc in section 54 as follows:

If any person, without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-

(a) accesses or secures access to such computer, computer system or computer network;

computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, or rules and regulations made there under;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network,

he shall be liable to pay to the person affected compensation not exceeding Taka one crore.

So this section provides penalty for damages as contravention, and section 56 provides the same parlance to hacking. However, both there sections should be brought in one section.

- **Hacking - whether Amounts to Theft and/or Criminal Trespass:** The Act of hacking under the ICT Act-2006 is nothing as a crime without the combination of criminal trespass and mischief of the Penal Code-1860.

According Section 425 of the Penal Code:

Whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility or affects it injuriously, commits mischief.

Applying the above sections to hacking would be correct if the following issue could be resolved unambiguously: whether information residing in a computer resource is "property" as envisaged by the Penal Code. And Computer Programme (CP) is one kind of copyrighted property under the Copyright Act- 2000.

According Section 441 of the Penal Code:

Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit criminal trespass.

- **Identity Theft:** Many Identity Theft offences happened on online purchases using falsifying credit card numbers by the accused. No provision exists to tackle this problem by the ICT Act-2006.

- **Immunity to Internet Service Providers (ISPs):** The Act gives immunity to Internet Service Providers or network service providers by stating that they will not be responsible or in charge if Acts in contravention of any provision of this Act are carried out using them as intermediaries. This is subject to them proving that, the offence or contravention was committed without his knowledge or that he had exercised due diligence to prevent the commission of such offence or contravention under section 79 of the ICT Act-2006. Although the immunity to ISPs helps to detect the real cyber criminals with the technical assistant, but cyber crime commission may increase for granting immunity of ISPs.

- **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 cyber crime under section 80 of the ICT Act-2006. 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 of being about to commit any offence under this Act'[24]. 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 cyber criminals, albeit cyber crime detection is very difficult. So, this is similar to section 54 of the Criminal Procedure Code in case of harassment to public.

- **Cyber Offences Investigating Police Officermust have Relevant Expertise:** Under section 80 of the ICT Act-2006 that a police officer not below the rank of an Inspector of Police shall investigate any offence under

[24] Section 79, the ICT Act, 2006.

penalties under section 84, which is very impractical unless cyber law related global agreement is in existence. This 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 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.

- **Electronic Payment:** The above shortcomings in the ICT Act-2006 disagree with the very objective of passing the Act encouraging e-commerce by giving it legal validity. But the ICT Act-2006 does not cover electronic payment. However, documents pertinent to negotiable instruments, (promissory notes, cheques, etc.) powers of attorney, trusts, wills, or other documents that the Government of Bangladesh may denote must be in a non-electronic form under section 2(1) of the Act. The filling up of forms, or the issue of a license, or payment of fee may also be in an electronic form under section 7 (1) and (2) of the Act. At the same time, no person can insist that a form or document should be in an electronic form or that a payment should be made electronically under section 10 of the ICT Act-2006. So, amendments to the Negotiable Instruments Act should be made to legalize the electronic payment (promissory notes, Acts of exchange and cheques, etc.). But the lack of provision for foreign currency handling is pointed out as a serious flaw in the draft law, which needs to be corrected before it is sent to the parliament for approval.

- **Section 54 of Cr. P.C. and Section 57 of ICT Act 2006:** Section 54 of the ICT Act-2006 replicates section 54 of the Criminal Procedure Code-1898, which gives more power to police. This empowered of police is treated as black law in the Bangladeshi legal system. Whereas it is a burning issue that section 54 should be omitted, but in the same time the ICT law has brought the provision as old wine in a new bottle. What countries like Bangladesh are doing is that they are blindly applying the provisions of the Criminal Procedure Code to the Internet without realizing that it is a different medium and not the real world.

- **Domain Names:** "Domain name" is the major issue, which relate 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 Property Rights of "domain name" owners. These need proper attentions.

penalties under section 84, which is very impractical unless cyber law related global agreement is in existence. This 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 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.

- **Electronic Payment:** The above shortcomings in the ICT Act-2006 disagree with the very objective of passing the Act encouraging e-commerce by giving it legal validity. But the ICT Act-2006 does not cover electronic payment. However, documents pertinent to negotiable instruments, (promissory notes, cheques, etc.) powers of attorney, trusts, wills, or other documents that the Government of Bangladesh may denote must be in a non-electronic form under section 2(1) of the Act. The filling up of forms, or the issue of a license, or payment of fee may also be in an electronic form under section 7 (1) and (2) of the Act. At the same time, no person can insist that a form or document should be in an electronic form or that a payment should be made electronically under section 10 of the ICT Act-2006. So, amendments to the Negotiable Instruments Act should be made to legalize the electronic payment (promissory notes, Acts of exchange and cheques, etc.). But the lack of provision for foreign currency handling is pointed out as a serious flaw in the draft law, which needs to be corrected before it is sent to the parliament for approval.

- **Section 54 of Cr. P.C. and Section 57 of ICT Act 2006:** Section 54 of the ICT Act-2006 replicates section 54 of the Criminal Procedure Code-1898, which gives more power to police. This empowered of police is treated as black law in the Bangladeshi legal system. Whereas it is a burning issue that section 54 should be omitted, but in the same time the ICT law has brought the provision as old wine in a new bottle. What countries like Bangladesh are doing is that they are blindly applying the provisions of the Criminal Procedure Code to the Internet without realizing that it is a different medium and not the real world.

- **Domain Names:** "Domain name" is the major issue, which relate 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 provision about the Intellectual

this Act. This section should be modified that Inspector of Police and above, must have appropriate ICT knowledge (i.e. Diploma/Bahelor's degree in ICT related subject/ proper training in this area).

- **Arrest without Warrant or not:** According to section 80 of the ICT Act-2006, a police officer has the power to search and arrest in any public places without warrant. But to search and arrest in any private places, a warrant is required which is time consuming and confidentially is compromised. As in the case of public places, search and arrest in any private places should be allowed without warrant with a letter of authorization from the concerned unit head.

- **Bureaucratization of Controlling e-Commerce Process:** The ICT Act-2006 provides the opportunity to use electronic records and digital signatures in government documents. But it further says in section 10 that there is no liability on Government to accept documents in electronic form. The control of the government is apparent which is described in section 18 as 'the Controller shall discharge such functions as are vested in him under this Act under the general superintendence and control of the Government.' This provision is necessary as electronic transactions are new in this country and many Government departments still lack the logistics to perform transactions in electronic form.[25] The ICT Act-2006 seeks to bureaucratize the intact process of controlling electronic commerce. This is likely to result into consequences of delays and other related problems.

- **Anti-Spamming Provision:** Spamming is an offence under the ICT Act-2006 in Bangladesh. Spamming is also a peril of the developed countries like USA, UK and other developed nations but the anti-spamming provisions should be omitted in very nascent stages e-commerce based countries like Bangladesh.

- **Implementation of Global Cyber Law:** Implementation of the law is a big question mark for any nations' law enforcing agency. The implementation of the global cyber law is a big challenge without any law enforcing agencies. But countries can take the lead in implementing the law within their national boundaries. Like the US, this has cyber squatting laws that make cyber squatting 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 citizens but also to any contravention or any violation done by anybody anywhere in the world is also liable to the

[25] Final Report on the Law of Information Technology, *loc. cit.*