**Cyber Crime in Bangladesh**

The emergence and usage of social networking websites is shaping lives in number of ways, both positive and negative. While the impact of ICT by way of making the planet a global village has pluses, on the dark side there is widespread misuse of ICT, right up to the excesses of cyber crime, cyber harassment and more.

Index

01. Introduction………………………………………………………………………………03

02. Cyber Crime……………………………………………………………………………...03

03. Major cyber Crimes……………………………………………………………………...03

a) Unauthorized access to a computer system………………………………………….04

b) Introduces or causes to introduce viruses……………………………………………04

c) Tampering with computer source documents………………………………………..04

d) Cause Damage to Computer system or causes any disruption………………………05

04. Real Scenario of Cyber Crime in Bangladesh………………………………………...…05

05. Prevention of cyber crime………………………………………………………………………..06

06. Law of Bangladesh about cyber crime…………………………………………………...07

07. Tribunal…………………………………………………………………………………..17

08. Conclution………………………………………………………………………………..18

09. Reference......................................................................................................................19

On 2012, Sabiha Sultana Sathi, a school girl of Bagerhaat who’s a friend takes her some personal photographs and broadens those on Internet. As a result Sathi committed suicide and this is not only Sathi’s story, a story of those girls who are the victim of cyber crime. Nowadays, cyber crime is a very common as well as a sevear crime all over the world. According to Bangladesh Police, cyber-crime take place every 20 seconds and over 500,000 web pages contain some form of hacker tool. Now the question arise what cyber crime? Well, Cyber crime refers to any crime that involves a computer and a network. Now let’s discuss about cyber crime briefly.

Cyber Crime:

Criminal offences committed against or with the help of computer networks is cyber crime. It is an offence against the confidentiality, integrity and availability of computer data and systems. The computer may have been used in the commission of a crime, or it may be the target. Dr. Debarati Halder and Dr. K. Jaishankar (2011) defines Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".

- Computer-related forgery

- Computer-related fraud

- Offences related to child pornography

- Offences related to infringements of copyright and related rights.

Major Cyber Crimes:

♣ Unauthorized access to a computer system.

♣ Introduces or causes to introduce viruses.

♣ Tampering with computer source documents.

♣ Cause Damage to Computer system or causes any disruption.

♣ Denies access to any person authorized to access the computer system.

Unauthorized access to a computer system:

Access to a computer system without the permission of the authorized person and depict his or her personal information to others which may cause defamation or harm to those person is a cyber crime. Unauthorized access to a computer system includes most of the cyber or net crime. For example-

- Illegal interception

- Data interference

- System interference

- Misuse of devices

Introduces or causes to introduce viruses:

Cyber crime often is a cause spread of viruses. Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. Through internet cyber offenders spread viruses among others computer to make them disable or work.

Tampering with computer source documents:

Issues surrounding these types of crimes have become high-profile, particularly those surrounding Cyber terrorism, Drug trafficking temper with computer source documents. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. The U.S. Department of Defense (DoD) notes that the cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia.

Cause Damage to Computer system or causes any disruption:

Cyber crime also does defamation of people. Many people specially the girls are the victim of cyber crime or cyber harassment. This harassment in cyber space has added new dimensions, going beyond typical day-to-day harassment. Such cyber harassment covers posting indecent pictures, lewd comments, obnoxious and humiliating message and so on. Major causes behind the harassment in the physical world and the cyberspaces are motley. In general, motivation of intimacy seeking, or refusal, revenge, peer pressures, odd social norms, poor implementation of laws and so on induce harassment in real world. On the contrary, virtual harassment is stimulated by attempts at making fun of the victim, or personal disputes, refusals, and the very nature and open-ended looseness of Internet use.

Real Scenario of Cyber Crime in Bangladesh:

Bangladesh has been carrying out anti- cyber crime activities from last year providing training for a group of professionals and developing software.

According to Deputy Inspector General (DIG) of the CID of the Police,

“As part of the strategy, the Crime Investigation Department (CID) o f t he Police would run a cyber crime laboratory later if its plan went accordingly.”

The DIG said by initiating the anti-cyber crime activities, Bangladesh had come to the age of combating high-tech crimes though no single cyber crime was recorded in the country. Earlier, Additional Inspector General of Police (IGP) NBK Tripura said Bangladesh's steps to combat the cyber crimes had been praised at home and abroad.

"Many of our friends’ from other countries have viewed that the steps are appropriate precautionary efforts,"

Tripura said adding that recently held three-day regional cyber crime seminar for the first time in November in Dhaka was a total success. Bangladesh had only 0.45 million Internet users in 2006 and the number of Internet hosts was 376 in 2007, according to available statistics. But the ratio of commercial users of Internet was significantly higher than household users. So, the law-enforcers should be prepared for resisting such high-tech crimes, which were usually taking place in the commercial sector, said another senior official. At present, the cyber crimes, including sending of porno pictures and cooked porno activities to achieve particular targets, may take place, but those were isolated events, and the number were very few, he said referring his crime intelligence report. Basically, no notable cyber crime has yet been committed in Bangladesh. The gradual dependence and extensive use of computer and information technology by the financial institutions like bank, insurance company, and other non-government organizations increase the fear of commission of cyber crime here. Computer has been used as a tool of crime like making forged certificates and documents for a number of years in Bangladesh though the incident of targeting computer or computer system is very unusual. Some of the incidents that bring the notice of the public are: E-mail threatening to the former Prime Minister

Sheikh Hasina from a cyber café, hacking the mail of BRAC Bangladesh, stealing the transaction report of Dhaka Stock Exchange through hacking, E-mail threatening to World Bank Dhaka Office and the President of the United States George Bush.

Prevention of cyber crime:

Prevention is always better than cure. It is always better to take certain precaution while operating the net. A should make them his part of cyber life. Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai PoliceCyber crime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance. A netizen should keep in mind thefollowing things-

1. To prevent cyber stalking avoid disclosing any information pertaining to one. This is as good as disclosing your identity to strangers in public place.

2. Always avoid sending any photograph online particularly to strangers and chatfriends as there have been incidents of misuse of the photographs.

3. Always use latest and up date anti virus software to guard against virus attacks.

4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination.

5. Never send your credit card number to any site that is not secured, to guard againstfrauds.6. Always keep a watch on the sites that your children are accessing to prevent anykind of harassment or depravation in children.

7. It is better to use a security programme that gives control over the cookies and sendinformation back to the site as leaving the cookies unguarded might prove fatal.

8. Web site owners should watch traffic and check any irregularity on the site. Puttinghost-based intrusion detection devices on servers may do this.

9. Use of firewalls may be beneficial.

10. Web servers running public sites must be physically separate protected frominternal corporate network.

Law of Bangladesh about cyber crime:

The various government across the globe are investing to bring the Police Force to meet the challenges of the Borderless Cyber Crime, Government of Bangladesh has also taken to make the Police Force e- Ready. In 2006 our Government also introduces an Act to prevent Cyber crime. That is তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (২০০৬ সনের ৩৯ নং আইন).

The Act is given below which deals with Cyber Crime-

অষ্টম অধ্যায়

অপরাধ, তদন্ত, বিচার, দন্ড ইত্যাদি

কম্পিউটার, কম্পিউটার সিস্টেম, ইত্যাদির অনিষ্ট সাধন ও দণ্ড ৫৪৷ (১) যদি কোন ব্যক্তি কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কের মালিক বা জিম্মাদারের অনুমতি ব্যতিরেকে-

(ক) উহার ফাইলে রতিগত তথ্য বিনষ্ট করিবার বা ফাইল হইতে তথ্য উদ্ধার বা সংগ্রহ করিবার উদ্দেশ্যে উক্ত কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে প্রবেশ করেন বা অন্য কোন ব্যক্তিকে প্রবেশ করিতে সহায়তা করেন;

(খ) কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক হইতে কোন উপাত্ত, উপাত্ত-ভাণ্ডার বা তথ্য বা উহার উদ্ধৃতাংশ সংগ্রহ করেন বা স্থানান্তরযোগ্য সংরতগণ ব্যবস্থায় রতিগত বা জমাকৃত তথ্য (removable storage medium) বা উপাত্তসহ উক্ত কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক এর তথ্য সংগ্রহ করেন বা কোন উপাত্তের অনুলিপি বা অংশ বিশেষ সংগ্রহ করেন;

(গ) কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে উদ্দেশ্যমূলকভাবে কোন ধরনের কম্পিউটার সংক্রামক বা দূষক বা কম্পিউটার ভাইরাস প্রবেশ করান বা প্রবেশ করানোর চেষ্টা করেন;

(ঘ) ইচ্ছাকৃতভাবে কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক, উপাত্ত, কম্পিউটারের উপাত্ত-ভাণ্ডারের ক্ষতিসাধন করেন বা ক্ষতিসাধনের চেষ্টা করেন বা উক্ত কম্পিউটার, সিস্টেম বা নেটওয়ার্কে রক্ষিত অন্য কোন প্রোগ্রামের ক্ষতি সাধন করেন বা করিবার চেষ্টা করেন;

(ঙ) ইচ্ছাকৃতভাবে কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা নেটওয়ার্কে বিঘ্ন সৃষ্টি করেন বা করিবার চেষ্টা করেন;

(চ) কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে কোন বৈধ বা ক্ষমতাপ্রাপ্ত ব্যক্তিকে কোন উপায়ে প্রবেশ করিতে বাধা সৃষ্টি করেন বা করিবার চেষ্টা করেন;

(ছ) এই আইন বা তদধীন প্রণীত বিধি বা প্রবিধানের কোন বিধান লঙ্ঘন করিয়া কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে কোন ব্যক্তিকে অবৈধ প্রবেশে সহায়তা প্রদান করেন;

(জ) ইচ্ছাকৃতভাবে প্রেরক বা গ্রাহকের অনুমতি ব্যতীত, কোন পণ্য বা সেবা বিপণনের উদ্দেশ্যে, স্পাম উত্পাদন বা বাজারজাত করেন বা করিবার চেষ্টা করেন বা অযাচিত ইলেক্ট্রনিক মেইল প্রেরণ করেন;

(ঝ) কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে অন্যায়ভাবে হস্তক্ষেপ বা কারসাজি করিয়া কোন ব্যক্তির সেবা গ্রহণ বাবদ ধার্য চার্জ অন্যের হিসাবে জমা করেন বা করিবার চেষ্টা করেন;

তাহা হইলে উক্ত ব্যক্তির উক্ত কার্য হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন অপরাধ করিলে তিনি ৩[ অনধিক চৌদ্দ বৎসর এবং অন্যূন সাত বৎসর কারাদণ্ডে], বা অনধিক দশ লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন৷

ব্যাখ্যাঃ এই ধারার উদ্দেশ্য পূরণকল্পে,-

(ক) ”কম্পিউটার দূষণ” অর্থ এমন সব কম্পিউটার নির্দেশনা যাহা নিম্নবর্ণিত কার্যের উদ্দেশ্যে প্রস্তুত করা হয়-

(অ) কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে রক্ষিত কোন রেকর্ড, উপাত্ত বা প্রোগ্রামের প্রেরণ বা সঞ্চারণ কার্যের পরিবর্তন বা বিনাশ সাধন;

(আ) যে কোন উপায়ে কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে স্বাভাবিক কার্যক্রমকে বাধাগ্রস্ত করা;

(খ) ”কম্পিউটার উপাত্ত-ভাণ্ডার” অর্থ টেক্সট, ইমেজ, অডিও বা ভিডিও আকারে উপস্থাপিত তথ্য জ্ঞান, ঘটনা, মৌলিক ধারণা বা নির্দেশাবলী, যাহা-

(অ) কোন কম্পিউটারের বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক দ্বারা আনুষ্ঠানিক পদ্ধতিতে প্রস্তুত হইতেছে বা হইয়াছে; এবং

(আ) কোন কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে ব্যবহারের উদ্দেশ্যে প্রস্তুত করা হইয়াছে;

(গ) ”কম্পিউটার ভাইরাস” অর্থ এমন কম্পিউটার নির্দেশ, তথ্য, উপাত্ত বা প্রোগ্রাম, যাহা-

(অ) কোন কম্পিউটার সম্পাদিত কার্যকে বিনাস, ক্ষতি বা ক্ষুণ্ন করে বা উহার কার্য-সম্পাদনের দক্ষতায় বিরূপ প্রভাব বিস্তার করে; বা

(আ) নিজেকে অন্য কোন কম্পিউটারের সহিত সংযুক্ত করিয়া উক্ত কম্পিউটারের কোন প্রোগ্রাম, উপাত্ত বা নির্দেশ কার্যকর করিবার বা কোন ক্রিয়া সম্পাদনের সময় নিজেই ক্রিয়াশীল হইয়া উঠে এবং উহার মাধ্যমে উক্ত কম্পিউটার কোন ঘটনা ঘটায়;

(ঘ) ”ক্ষতি” অর্থ এমন কোন কার্য যাহার দ্বারা কোন কম্পিউটারে রক্ষিত তথ্য বা উপাত্ত বিনষ্ট, পরিবর্তন, সংযোজন, সংশোধন বা পুনঃবিন্যাস করা হয় বা মুছিয়া ফেলা হয়৷

কম্পিউটার সোর্স কোড পরিবর্তন সংক্রান্ত অপরাধ ও উহার দণ্ড ৫৫৷ কোন ব্যক্তি যদি ইচ্ছাকৃতভাবে বা জ্ঞাতসারে, কোন কম্পিউটার, কম্পিউটার প্রোগ্রাম, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে ব্যবহৃত কম্পিউটার সোর্স কোড, গোপন, ধ্বংস বা পরিবর্তন করেন, বা অন্য কোন ব্যক্তির মাধ্যমে উক্ত কোড, প্রোগ্রাম, সিস্টেম বা নেটওয়ার্ক গোপন, ধ্বংস বা পরিবর্তন করিবার চেষ্টা করেন এবং উক্ত সোর্স কোডটি যদি আপাততঃ বলবত্ অন্য কোন আইন দ্বারা সংরক্ষণযোগ্য বা রক্ষণাবেক্ষণযোগ্য হয়, তাহা হইলে তাহার এই কাজ হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন কোন অপরাধ করিলে তিনি অনধিক তিন বত্সর কারাদণ্ডে, বা অনধিক তিন লক্ষ টাকা অর্থদণ্ড, বা উভয় দণ্ডে দণ্ডিতে হইবেন৷

ব্যাখ্যাঃ এই ধারার উদ্দেশ্য পূরণকল্পে, “কম্পিউটার সোর্স কোড” অর্থ তালিকাভুক্ত প্রোগ্রাম, কম্পিউটার কমান্ড, ডিজাইন ও লে-আইট তালিকাভুক্তি এবং কম্পিউটার রিসোর্সের যে কোন ধরনের প্রোগ্রাম বিশ্লেষণ৷

কম্পিউটার সিস্টেমের হ্যাকিং সংক্রান্ত অপরাধ ও উহার দণ্ড ৫৬৷ (১) কোন ব্যক্তি যদি-

(ক) জনসাধারণের বা কোন ব্যক্তির ক্ষতি করিবার উদ্দেশ্যে বা ক্ষতি হইবে মর্মে জ্ঞাত হওয়া সত্ত্বেও এমন কোন কার্য করেন যাহার ফলে কোন কম্পিউটার রিসোর্সের কোন তথ্য বিনাশ, বাতিল বা পরিবর্তিত হয় বা উহার মূল্য বা উপযোগিতা হ্রাস পায় বা অন্য কোনভাবে উহাকে ক্ষতিগ্রস্ত করে;

(খ) এমন কোন কম্পিউটার, সার্ভার, কম্পিউটার নেটওয়ার্ক বা অন্য কোন ইলেক্ট্রনিক সিস্টেমে অবৈধভাবে প্রবেশ করার মাধ্যমে ইহার ক্ষতিসাধন করেন, যাহাতে তিনি মালিক বা দখলকার নহেন;

তাহা হইলে তাহার এই কার্য হইবে একটি হ্যাকিং অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন হ্যাকিং অপরাধ করিলে তিনি ৪[ অনধিক চৌদ্দ বৎসর এবং অন্যূন সাত বৎসর কারাদণ্ডে], বা অনধিক এক কোটি টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন৷

ইলেক্ট্রনিক ফরমে মিথ্যা, অশ্লীল অথবা মানহানিকর তথ্য প্রকাশ সংক্রান্ত অপরাধ ও উহার দণ্ড ৫৭৷ (১) কোন ব্যক্তি যদি ইচ্ছাকৃতভাবে ওয়েব সাইটে বা অন্য কোন ইলেক্ট্রনিক বিন্যাসে এমন কিছু প্রকাশ বা সম্প্রচার করেন, যাহা মিথ্যা ও অশ্লীল বা সংশ্লিষ্ট অবস্থা বিবেচনায় কেহ পড়িলে, দেখিলে বা শুনিলে নীতিভ্রষ্ট বা অসৎ হইতে উদ্বুদ্ধ হইতে পারেন অথবা যাহার দ্বারা মানহানি ঘটে, আইন শৃঙ্খলার অবনতি ঘটে বা ঘটার সম্ভাবনা সৃষ্টি হয়, রাষ্ট্র ও ব্যক্তির ভাবমূর্তি ক্ষুণ্ন হয় বা ধর্মীয় অনুভূতিতে আঘাত করে বা করিতে পারে বা এ ধরনের তথ্যাদির মাধ্যমে কোন ব্যক্তি বা সংগঠনের বিরুদ্ধে উস্কানী প্রদান করা হয়, তাহা ইহলে তাহার এই কার্য হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন অপরাধ করিলে তিনি ৫[ অনধিক চৌদ্দ বৎসর এবং অন্যূন সাত বৎসর কারাদণ্ডে] এবং অনধিক এক কোটি টাকা অর্থদণ্ডে দণ্ডিত হইবেন৷

লাইসেন্স সমর্পণে ব্যর্থতা ও উহার দণ্ড ৫৮৷ (১) ধারা ৩৪ এর অধীন কোন সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ যদি কোন লাইসেন্স সমর্পণ করিতে ব্যর্থ হয়, তাহা হইলে যে ব্যক্তির অনুকূলে উক্ত লাইসেন্স প্রদান করা হইয়াছিল সেই ব্যক্তির উক্ত ব্যর্থতা হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন অপরাধ করিলে তিনি অনধিক ছয় মাস কারাদণ্ডে, বা অনধিক দশ হাজার টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন৷

নির্দেশ লঙ্ঘন সংক্রান্ত অপরাধ ও উহার দণ্ড ৫৯৷ (১) এই আইন বা তদধীন প্রণীত বিধি বা প্রবিধানের কোন বিধান প্রতিপালন নিশ্চিত করিবার প্রয়োজনে নিয়ন্ত্রক, আদেশ দ্বারা, কোন সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ বা উহার কোন কর্মচারীকে আদেশে উল্লিখিতমতে কোন বিষয়ে ব্যবস্থা গ্রহণ করিতে বা কোন কার্য করা হইতে বিরত থাকিতে নির্দেশ প্রদান করিলে কোন ব্যক্তি যদি উক্ত নির্দেশ লংঘন করেন, তাহা হইলে উক্ত লংঘন হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন অপরাধ করিলে তিনি অনধিক এক বৎসর কারাদণ্ডে, বা অনধিক এক লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন৷

জরুরী পরিস্থিততে নিয়ন্ত্রকের নির্দেশ অমান্যে দণ্ড ৬০৷ (১) বাংলাদেশের সার্বভৌমত্ব, অখণ্ডতা, নিরাপত্তা, অন্যান্য বিদেশী রাষ্ট্রের সহিত বাংলাদেশের বন্ধুত্বপূর্ণ সম্পর্ক, জনশৃঙ্খলা ও নিরাপত্তা রক্ষার স্বার্থে বা এই আইনের অধীন দণ্ডযোগ্য কোন অপরাধ সংঘটনের প্ররোচনা প্রতিরোধের জন্য নিয়ন্ত্রক, লিখিত আদেশ দ্বারা, সরকারের কোন আইন প্রণয়নকারী সংস্থাকে কোন কম্পিউটার রিসোর্সের মাধ্যমে কোন তথ্য সম্প্রচারে বাধা দেওয়ার নির্দেশ প্রদান করিলে কোন ব্যক্তি অনুরূপ বাধা অমান্য করিয়া কোন তথ্য সম্প্রচার করিলে উহা হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন অপরাধ করিলে তিনি অনধিক পাঁচ বৎসর কারাদণ্ডে, বা অনধিক পাঁচ লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন৷

সংরক্ষিত সিস্টেমে প্রবেশ সংক্রান্ত অপরাধ ও উহার দণ্ড ৬১৷ (১) নিয়ন্ত্রক, সরকারী বা ঐচ্ছিকভাবে ইলেক্ট্রনিক গেজেটে প্রজ্ঞাপন দ্বারা, কোন কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ককে একটি সংরক্ষিত সিস্টেম হিসাবে ঘোষণা করা সত্ত্বেও যদি কোন ব্যক্তি উক্ত সংরক্ষিত কম্পিউটার, সিস্টেম বা নেটওয়ার্কে অননুমোদিতভাবে প্রবেশ করেন, তাহা হইলে তাহার এই অননুমোদিত প্রবেশ হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন কোন অপরাধ করিলে তিনি ৬[ অনধিক চৌদ্দ বৎসর এবং অন্যূন সাত বৎসর কারাদণ্ডে], বা অনধিক দশ লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন৷

মিথ্যা প্রতিনিধিত্ব ও তথ্য গোপন সংক্রান্ত অপরাধ ও উহার দণ্ড ৬২৷ (১) যদি কোন ব্যক্তি লাইসেন্স বা ইলেক্ট্রনিক স্বাতগর সার্টিফিকেট প্রাপ্তির জন্য নিয়ন্ত্রক বা সার্টিফিকেট প্রদানকারী কর্তৃপতেগর নিকট মিথ্যা পরিচয় প্রদান করেন বা কোন গুরুত্বপূর্ণ তথ্য গোপন করেন, তাহা হইলে তাহার উক্ত কার্য হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন অপরাধ করিলে তিনি অনধিক দুই বৎসর কারাদণ্ডে, বা অনধিক দুই লক্ষ টাকা অর্থদণ্ডে, বা উভয়দণ্ডে দণ্ডিত হইবেন৷

গোপনীয়তা প্রকাশ সংক্রান্ত অপরাধ ও উহার দণ্ড ৬৩৷ (১) এই আইন বা আপাততঃ বলবত্ অন্য কোন আইনে ভিন্নরূপ কোন কিছু না থাকিলে, কোন ব্যক্তি যদি এই আইন বা তদধীন প্রণীত বিধি বা প্রবিধানের কোন বিধানের অধীন কোন ইলেক্ট্রনিক রেকর্ড, বই, রেজিস্টার, পত্রযোগাযোগ, তথ্য, দলিল বা অন্য কোন বিষয়বস্তুতে প্রবেশাধিকারপ্রাপ্ত হইয়া, সংশ্লিষ্ট ব্যক্তির সম্মতি ব্যতিরেকে, কোন ইলেক্ট্রনিক রেকর্ড, বই, রেজিস্টার, পত্রযোগাযোগ, তথ্য, দলিল বা অন্য কোন বিষয়বস্তু অন্য কোন ব্যক্তির নিকট প্রকাশ করেন, তাহা হইলে তাহার এই কার্য হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন অপরাধ করিলে তিনি অনধিক দুই বৎসর কারাদণ্ডে, বা অনধিক দুই লক্ষ টাকা অর্থদণ্ডে, বা উভয়দণ্ডে দণ্ডিত হইবেন৷

ভুয়া (false) ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রকাশ সংক্রান্ত অপরাধ ও দণ্ড ৬৪৷ (১) কোন ব্যক্তি ইচ্ছাকৃতভাবে নিম্নবর্ণিত বিষয়ে কোন ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রকাশ বা অন্য কোনভাবে অন্য কোন ব্যক্তির প্রাপ্তিসাধ্য করিবেন না, যাহা-

(ক) তালিকাভুক্ত সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ কর্তৃক ইস্যুকৃত হয় নাই; বা

(খ) তালিকাভুক্ত গ্রাহক কর্তৃক উহা গৃহীত হয় নাই; বা

(গ) বাতিল বা স্থগিত করা হইয়াছে;

যদি না উক্ত প্রকাশনা কোন ইলেক্ট্রনিক স্বাক্ষর বাতিল বা স্থগিতের পূর্বেই যাচাইয়ের উদ্দেশ্যে তৈরি করা হইয়া থাকে এবং যদি উক্ত বিধান লংঘনক্রমে উক্ত সার্টিফিকেট প্রকাশ বা অন্য কোনভাবে অন্য কোন ব্যক্তির প্রাপ্তিসাধ্য করেন, তাহা হইলে তাহার এই কার্য হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন অপরাধ করিলে তিনি অনধিক দুই বৎসর কারাদণ্ডে, বা অনধিক দুই লক্ষ টাকা অর্থদণ্ডে, বা উভয়দণ্ডে দণ্ডিত হইবেন৷

প্রতারণার উদ্দেশ্যে ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রকাশ, ইত্যাদি সংক্রান্ত অপরাধ ও উহার দণ্ড ৬৫৷ (১) যদি কোন ব্যক্তি ইচ্ছাকৃতভাবে প্রতারণা বা অন্য কোন বে-আইনী উদ্দেশ্যে কোন ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রস্তুত, প্রকাশ বা প্রাপ্তিসাধ্য করেন, তাহা হইলে তাহার এই কার্য হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন কোন অপরাধ করিলে তিনি অনধিক দুই বৎসর কারাদণ্ডে, বা অনধিক দুই লক্ষ টাকা অর্থদণ্ডে, বা উভয়দণ্ডে দণ্ডিত হইবেন৷

কম্পিউটার ব্যবহারের মাধ্যমে অপরাধ সংঘটন ও উহার দণ্ড ৬৬৷ (১) যদি কোন ব্যক্তি ইচ্ছাকৃতভাবে কোন কম্পিউটার, ই-মেইল বা কম্পিউটার নেটওয়ার্ক, রিসোর্স বা সিস্টেম ব্যবহারের মাধ্যমে এই আইনের অধীন কোন অপরাধ সংঘটনে সহায়তা করেন, তাহা হইলে তাহার উক্ত কার্য হইবে একটি অপরাধ৷

(২) কোন ব্যক্তি উপ-ধারা (১) এর অধীন কোন অপরাধ সংঘটনে সহায়তা করিবার ক্ষেতে মূল অপরাধটির জন্য যে দণ্ড নির্ধারিত রহিয়াছে তিনি সেই দণ্ডেই দণ্ডিত হইবেন৷

কোম্পানী, ইত্যাদি কর্তৃক অপরাধ সংঘটন ৬৭৷ কোন কোম্পানী কর্তৃক এই আইনের অধীন কোন অপরাধ সংঘটিত হইলে উক্ত অপরাধের সহিত প্রত্যক্ষ সংশ্লিষ্টতা রহিয়াছে কোম্পানীর এমন প্রত্যেক পরিচালক, ম্যানেজার, সচিব, অংশীদার, কর্মকর্তা এবং কর্মচারী উক্ত অপরাধ সংঘটিত করিয়াছেন বলিয়া গণ্য হইবেন, যদি না প্রমাণ করা যায় যে, উক্ত অপরাধ তাহার অজ্ঞাতসারে সংঘটিত হইয়াছে অথবা উক্ত অপরাধ রোধ করিবার জন্য তিনি যথাসাধ্য চেষ্টা করিয়াছেন৷

ব্যাখ্যাঃ এই ধারায়-

(ক) “কোম্পানী” বলিতে কোন বাণিজ্যিক প্রতিষ্ঠান, অংশীদারী কারবার, সমিতি, সংঘ এবং সংগঠনও অন্তর্ভুক্ত হইবে; এবং

(খ) বাণিজ্যিক প্রতিষ্ঠানের ক্ষেত্রে “পরিচালক” বলিতে উহার কোন অংশীদার বা পরিচালনা বোর্ডের সদস্যকেও বুঝাইবে৷

সাইবার ট্রাইব্যুনাল গঠন ৬৮৷ (১) সরকার, সরকারী গেজেটে প্রজ্ঞাপন দ্বারা, এই আইনের অধীন সংঘটিত অপরাধের দ্রুত ও কার্যকর বিচারের উদ্দেশ্যে, এক বা একাধিক সাইবার ট্রাইব্যুনাল, অতঃপর সময় সময় ট্রাইব্যুনাল বলিয়া উল্লিখিত, গঠন করিতে পারিবে৷

(২) উপ-ধারা (১) এর অধীন গঠিত সাইবার ট্রাইব্যুনাল সুপ্রীম কোর্টের সহিত পরামর্শক্রমে, সরকার কর্তৃক নিযুক্ত একজন দায়রা জজ বা একজন অতিরিক্ত দায়রা জজের সমন্বয়ে গঠিত হইবে; এবং অনুরূপভাবে নিযুক্ত একজন বিচারক “বিচারক, সাইবার ট্রাইব্যুনাল” নামে অভিহিত হইবেন৷

(৩) এই ধারার অধীন গঠিত সাইবার ট্রাইব্যুনালকে সমগ্র বাংলাদেশের স্থানীয় অধিক্ষেত্র অথবা এক বা একাধিক দায়রা ডিভিশনের অধিক্ষেত্র প্রদান করা যাইতে পারে; এবং উক্ত ট্রাইব্যুনাল কেবল এই আইনের অধীন অপরাধের মামলার বিচার করিবে৷

(৪) সরকার কর্তৃক পরবর্তীতে গঠিত কোন ট্রাইব্যুনালকে সমগ্র বাংলাদেশের অথবা এক বা একাধিক দায়রা বিভাগের সমন্বয়ে গঠিত উহার অংশ বিশেষের স্থানীয় অধিক্ষেত্র ন্যস্ত করিবার কারণে ইতঃপূর্বে কোন দায়রা আদালতে এই আইনের অধীন নিস্পন্নাাধীন মামলার বিচার কার্যক্রম স্থগিত, বা সংশ্লিষ্ট স্থানীয় অধিক্ষেত্রের ট্রাইব্যুনালে স্বয়ংক্রিয়ভাবে বদলী হইবে না, তবে সরকার, সরকারী গেজেটে প্রজ্ঞাপন দ্বারা, দায়রা আদালতে নিষ্পন্নাধীন এই আইনের অধীন কোন মামলা বিশেষ স্থানীয় অধিক্ষেত্রসম্পন্ন ট্রাইব্যুনালে বদলী করিতে পারিবে৷

(৫) কোন ট্রাইব্যুনাল, ভিন্নরূপ সিদ্ধান্ত গ্রহণ না করিলে, যে সাক্ষীর সাক্ষ্য গ্রহণ করা হইয়াছে উক্ত সাক্ষীর সাক্ষ্য পুনঃগ্রহণ, বা পুনঃশুনানী গ্রহণ করিতে, অথবা উপ-ধারা (৪) এর অধীন গৃহীত কার্যধারা পুনরায় আরম্ভ করিতে বাধ্য থাকিবে না, তবে ট্রাইব্যুনাল ইতোমধ্যে যে সাক্ষ্য গ্রহণ বা উপস্থাপন করা হইয়াছে উক্ত সাক্ষের ভিত্তিতে কার্য করিতে এবং মামলা যে পর্যায়ে ছিল সেই পর্যায় হইতে বিচারকার্য অব্যাহত রাখিতে পারিবে৷

(৬) সরকার, আদেশ দ্বারা, যে স্থান বা সময় নির্ধারণ করিবে সেই স্থান বা সময়ে বিশেষ ট্রাইব্যুনাল আসন গ্রহণ করিতে পারিবে এবং উহার কার্যক্রম পরিচালনা করিতে পারিবে৷

সাইবার ট্রাইব্যুনালের বিচার পদ্ধতি ৬৯৷ (১) সাব-ইন্সপেক্টর পদমর্যাদার নিম্নে নহে এইরূপ কোন পুলিশ কর্মকর্তার লিখিত রিপোর্ট ৭[ অথবা] নিয়ন্ত্রক বা তদুদ্দেশ্যে তাহার নিকট হইতে ক্ষমতাপ্রাপ্ত কোন কর্মকর্তার পূর্বানুমোদন ব্যতীত বিশেষ ট্রাইব্যুনাল কোন অপরাধ বিচারার্থ গ্রহণ করিবে না৷

(২) ট্রাইব্যুনাল এই আইনের অধীন অপরাধের বিচারকালে দায়রা আদালতে বিচারের জন্য ফৌজদারী কার্যবিধির অধ্যায় ২৩ এর বর্ণিত পদ্ধতি, এই আইনের বিধানাবলীর সহিত অসংগতিপূর্ণ না হওয়া সাপেক্ষে, অনুসরণ করিবে৷

(৩) কোন ট্রাইব্যুনাল, ন্যায়বিচারের স্বার্থে প্রয়োজনীয় না হইলে, এবং কারণ লিখিতভাবে লিপিবদ্ধ না করিয়া, কোন মামলার বিচারকার্য স্থগিত করিতে পারিবে না৷

(৪) যেইক্ষেত্রে ট্রাইব্যুনালের বিশ্বাস করিবার কারণ থাকে যে, অভিযুক্ত ব্যক্তি পলাতক রহিয়াছেন বা আত্মগোপন করিয়াছেন যে কারণে তাহাকে গ্রেপ্তার করিয়া বিচারের জন্য উপস্থিত করা সম্ভব নহে এবং তাহাকে অবিলম্বে গ্রেপ্তারের অবকাশ নাই, সেইক্ষেত্রে উক্ত ট্রাইব্যুনাল, আদেশ দ্বারা, বহুল প্রচারিত অন্যান্য জাতীয় দুইটি বাংলা দৈনিক সংবাদপত্রে, অনুরূপ ব্যক্তিকে আদেশে উল্লিখিত সময়ের মধ্যে হাজির হইবার নির্দেশ প্রদান করিতে পারিবে, এবং উক্ত ব্যক্তি অনুরূপ নির্দেশ পালন করিতে ব্যর্থ হইলে তাহার অনুপস্থিতিতেই তাহার বিচার করা হইবে৷

(৫) ট্রাইব্যুনালের সামনে অভিযুক্ত ব্যক্তি উপস্থিত হইবার বা জামিনে মুক্তি পাইবার পর পলাতক হইলে অথবা উহার সম্মুখে উপস্থিত হইতে ব্যর্থ হইলে, উপ-ধারা (৪) এ উল্লিখিত পদ্ধতি প্রযোজ্য হইবে না, এবং উক্ত ট্রাইব্যুনাল উহার সিদ্ধান্ত লিপিবদ্ধ করিয়া অনুরূপ ব্যক্তির অনুপস্থিতিতেই বিচার করিবে৷

(৬) ট্রাইব্যুনাল, উহার নিকট পেশকৃত আবেদনের ভিত্তিতে, বা উহার নিজ উদ্যোগে, কোন পুলিশ কর্মকর্তা বা, ক্ষেত্রমত, নিয়ন্ত্রক বা এতদুদ্দেশ্যে নিয়ন্ত্রকের নিকট হইতে ক্ষমতাপ্রাপ্ত কোন কর্মকর্তাকে এই আইনের অধীন সংঘটিত অপরাধ সংশ্লিষ্ট যে কোন মামলা পুনঃতদন্তের, এবং তদ্কর্তৃক নির্ধারিত সময়ের মধ্যে রিপোর্ট প্রদানের নিদের্শ প্রদান করিতে পারিবে৷

ট্রাইব্যুনালের কার্যক্রমে ফৌজদারী কার্যবিধির প্রয়োগ ৭০৷ (১) ফৌজদারী কার্যবিধির বিধানাবলী, যতদূর সম্ভব, এই আইনের বিধানাবলীর সহিত অসংগতিপূর্ণ না হওয়া সাপেক্ষে, ট্রাইব্যুনালের কার্যক্রমে প্রযোজ্য হইবে, এবং আদি এখতিয়ার প্রয়োগকারী দায়রা আদালতের সকল ক্ষমতা উক্ত ট্রাইব্যুনালের থাকিবে৷

(২) ট্রাইব্যুনালে সরকার পক্ষে মামলা পরিচালনাকারী ব্যক্তি পাবলিক প্রসিকিউটর বলিয়া গণ্য হইবেন৷

জামিন সংক্রান্ত বিধান ৭১৷ সাইবার ট্রাইব্যুনালের বিচারক এই আইনের অধীন দণ্ডযোগ্য কোন অপরাধে অভিযুক্ত ব্যক্তিকে জামিনে মুক্তি প্রদান করিবেন না, যদি না-

(ক) রাষ্ট্রপক্ষকে অনুরূপ জামিনের আদেশের উপর শুনানীর সুযোগ প্রদান করা হয়;

(খ) বিচারক সন্তুষ্ট হন যে,-

(অ) অভিযুক্ত ব্যক্তি বিচারে দোষী সাব্যস্ত নাও হইতে পারেন মর্মে বিশ্বাস করিবার যুক্তিসঙ্গত কারণ রহিয়াছে;

(আ) অপরাধ আপেক্ষিক অর্থে গুরুতর নহে এবং অপরাধ প্রমাণিত হইলেও শাস্তি কঠোর হইবে না; এবং

(গ) তিনি অনুরূপ সস্তুষ্টির কারণসমূহ লিখিতভাবে লিপিবদ্ধ করেন৷

রায় প্রদানের সময়সীমা ৭২৷ (১) ট্রাইব্যুনালের বিচারক সাক্ষ্য অথবা যুক্তিতর্ক সমাপ্ত হইবার তারিখ হইতে, যাহা পরে ঘটে, দশ দিনের মধ্যে রায় প্রদান করিবেন, যদি না তিনি লিখিতভাবে কারণ লিপিবদ্ধ করিয়া উক্ত সময়সীমা অনধিক দশ দিন বৃদ্ধি করেন৷

(২) উপ-ধারা (১) এর অধীন ট্রাইব্যুনাল কর্তৃক রায় প্রদান করা হইলে বা উক্ত রায়ের অধীন সাইবার আপীল ট্রাইব্যুনালে কোন আপীল দায়ের হইলে উক্ত আপীলের রায়ের কপি ধারা ১৮(৭) এর অধীন গঠিত ইলেক্ট্রনিক রেকর্ড সংরক্ষণ কক্ষে সংরক্ষণের উদ্দেশ্যে সংশ্লিষ্ট ট্রাইব্যুনাল বা সাইবার আপীল ট্রাইব্যুনাল উহার রায়ের কপি নিয়ন্ত্রকের নিকট প্রেরণ করিবে; উক্তরূপে কোন রায়ের কপি প্রেরণ করা হইলে, নিয়ন্ত্রক উহা উক্ত কক্ষে সংরক্ষণের যথাযথ ব্যবস্থা গ্রহণ করিবেন৷

ট্রাইব্যুনাল কর্তৃক মামলা নিষ্পত্তির নির্ধারিত সময়সীমা ৭৩৷ (১) ট্রাইব্যুনালের বিচারক মামলার অভিযোগ গঠনের তারিখ হইতে ছয় মাসের মধ্যে মামলার বিচার কার্য সমাপ্ত করিবেন৷

(২) বিচারক উপ-ধারা (১) এর অধীন নির্ধারিত সময়ের মধ্যে কোন মামলা নিষ্পত্তি করিতে ব্যর্থ হইলে, তিনি উহার কারণ লিখিতভাবে লিপিবদ্ধ করিয়া সময়সীমা অনধিক আরও তিন মাস বৃদ্ধি করিতে পারিবেন৷

(৩) উপ-ধারা (২) এর অধীন নির্ধারিত সময়ের মধ্যে বিচারক কোন মামলার নিষ্পত্তি করিতে ব্যর্থ হইলে, তিনি উহার কারণ লিপিবদ্ধ করিয়া বিষয়টি প্রতিবেদন আকারে হাইকোর্ট বিভাগ ও নিয়ন্ত্রককে অবহিত করিয়া মামলার কার্যক্রম পরিচালনা অব্যাহত রাখিতে পারিবেন৷

দায়রা আদালত কর্তৃক অপরাধের বিচার ৭৪৷ ফৌজদারী কার্যবিধিতে যাহা কিছুই থাকুক না কেন, এতদুদ্দেশ্যে বিশেষ ট্রাইব্যুনাল গঠিত না হওয়া পর্যন্ত এই আইনের অধীন অপরাধসমূহ দায়রা আদালত কর্তৃক বিচার্য হইবে৷

দায়রা আদালত কর্তৃক অনুসরণীয় বিচার পদ্ধতি ৭৫৷ (১) দায়রা আদালত এই আইনের অধীন অপরাধ বিচারের সময় দায়রা আদালতে বিচারের ক্ষেত্রে প্রযোজ্য ফৌজদারী কার্যবিধির অধ্যায় ২৩ এ বর্ণিত পদ্ধতি অনুসরণ করিবে৷

(২) ফৌজদারী কার্যবিধিতে যাহা কিছুই থাকুক না কেন, সাব-ইন্সপেক্টর পদমর্যাদার নিম্নে নহে এইরূপ পুলিশ কর্মকর্তার লিখিত রিপোর্ট ৮[ অথবা] নিয়ন্ত্রক কিংবা এতদুদ্দেশ্যে তাহার নিকট হইতে ক্ষমতাপ্রাপ্ত কোন কর্মকর্তার পূর্বানুমোদন ব্যতিরেকে কোন দায়রা আদালত আদি এখতিয়ার সম্পন্ন আদালত হিসাবে, এই আইনের অধীন কোন অপরাধ বিচারার্থ গ্রহণ করিবে না৷

অপরাধ তদন্তের ক্ষমতা, ইত্যাদি ৭৬৷ (১) ফৌজদারী কার্যবিধিতে যাহা কিছুই থাকুক না কেন, নিয়ন্ত্রক বা নিয়ন্ত্রক হইতে এতদুদ্দেশ্যে ক্ষমতাপ্রাপ্ত কোন কর্মকর্তা বা সাব-ইন্সপেক্টরের পদমর্যাদার নিম্নে নহেন এমন কোন পুলিশ কর্মকর্তা এই আইনের অধীন কোন অপরাধ তদন্ত করিবেন৷

৯[ (১ক) উপ-ধারা (১) এ যাহা কিছুই থাকুক না কেন, নিয়ন্ত্রক বা তদ্কর্তৃক ক্ষমতাপ্রাপ্ত কোন কর্মকর্তা বা উক্ত উপ-ধারায় উল্লিখিত কোন পুলিশ কর্মকর্তা কর্তৃক এই আইনের অধীন কোন অপরাধ একই সাথে তদন্ত করা যাইবে না।

(১খ) কোন মামলার তদন্তের যে কোন পর্যায়ে যদি প্রতীয়মান হয় যে, উক্ত মামলার সুষ্ঠু তদন্তের স্বার্থে, তদন্ত পরিচালনার দায়িত্ব-

(ক) পুলিশ কর্মকর্তার নিকট হইতে নিয়ন্ত্রক বা তদ্কর্তৃক ক্ষমতাপ্রাপ্ত কর্মকর্তা, বা

(খ) নিয়ন্ত্রক বা তদ্কর্তৃক ক্ষমতাপ্রাপ্ত কর্মকর্তার নিকট হইতে পুলিশ কর্মকর্তার, নিকট হস্তান্তর করা প্রয়োজন, তাহা হইলে সরকার বা, ক্ষেত্রমত, সাইবার ট্রাইব্যুনাল, আদেশ দ্বারা, পুলিশ কর্মকর্তার নিকট হইতে নিয়ন্ত্রক বা তদ্কর্তৃক ক্ষমতাপ্রাপ্ত কর্মকর্তার নিকট অথবা নিয়ন্ত্রক বা তদ্কর্তৃক ক্ষমতাপ্রাপ্ত কর্মকর্তার নিকট হইতে পুলিশ কর্মকর্তার নিকট হস্তান্তর করিতে পারিবে।]

১০[ (২) ধারা –

(ক) ৫৪, ৫৬, ৫৭, ও ৬১ এ উল্লিখিত অপরাধসমূহ আমলযোগ্য (Cognizable) ও অ-জামিনযোগ্য হইবে; এবং

(খ) ৫৫, ৫৮, ৫৯, ৬০, ৬২, ৬৩, ৬৪ ও ৬৫ এ উল্লিখিত অপরাধসমূহ অ-আমলযোগ্য (non-cognizable) ও জামিনযোগ্য হইবে;]

বাজেয়াপ্তি ৭৭৷ (১) এই আইনের অধীন কোন অপরাধ সংঘটিত হইলে, যে কম্পিউটার, কম্পিউটার সিস্টেম, ফ্লপি, কমপ্যাক্ট ডিস্ক (সিডি), টেপ ড্রাইভ বা অন্য কোন আনুষঙ্গিক কম্পিউটার উপকরণ বা বস্তু সম্পর্কে বা সহযোগে উক্ত অপরাধ সংঘটিত হইয়াছে সেইগুলি উক্ত অপরাধের বিচারকারী আদালতের আদেশানুসারে বাজেয়াপ্তযোগ্য হইবে৷

(২) যদি আদালত এই মর্মে সন্তুষ্ট হয় যে, যে ব্যক্তির দখল বা নিয়ন্ত্রণে উক্ত কম্পিউটার, কম্পিউটার সিস্টেম, ফ্লপি ডিক্স, কমপ্যাক্ট ডিস্ক, বা অন্য কোন আনুষঙ্গিক কম্পিউটার উপকরণ পাওয়া গিয়াছে তিনি এই আইন বা তদধীন প্রণীত বিধি বা প্রবিধানের কোন বিধান লংঘনের জন্য বা অপরাধ সংঘটনের জন্য দায়ী নহেন, তাহা হইলে উক্ত কম্পিউটার, কম্পিউটার সিস্টেম, ফ্লপি ডিস্ক, কমপ্যাক্ট ডিক্স, টেপ ড্রাইভ বা অন্য কোন আনুষঙ্গিক কম্পিউটার উপকরণ বাজেয়াপ্তযোগ্য হইবে না৷

(৩) উপ-ধারা (১) এর অধীন বাজেয়াপ্তযোগ্য কোন কম্পিউটার, কম্পিউটার সিস্টেম, ফ্লপি ডিস্ক, কমপ্যাক্ট ডিস্ক, টেপ ড্রাইভ বা অন্য কোন আনুষঙ্গিক কম্পিউটার উপকরণের সহিত কোন বৈধ কম্পিউটার, কম্পিউটার সিস্টেম, ফ্লপি ডিস্ক, কমপ্যাক্ট ডিস্ক, টেপ ড্রাইভ বা অন্য কোন কম্পিউটার উপকরণ পাওয়া যায়, তাহা হইলে সেইগুলিও বাজেয়াপ্তযোগ্য হইবে৷

(৪) এই ধারায় যাহা কিছুই থাকুক না কেন, উপ-ধারা (১) এ উল্লিখিত কোন অপরাধ সংঘটনের জন্য যদি কোন সরকারী বা সংবিধিবদ্ধ সরকারী কর্তৃপক্ষের কোন কম্পিউটার বা তৎসংশ্লিষ্ট কোন উপকরণ বা যন্ত্রপাতি ব্যবহার করা হয়, তাহা হইলে উহা বাজেয়াপ্তযোগ্য হইবে না৷

দণ্ড বা বাজেয়াপ্তকরণ অন্য কোন শাস্তি প্রদানে বাধা না হওয়া ৭৮৷ এই আইনের অধীন প্রদত্ত দণ্ড বা বাজেয়াপ্তকরণ আদেশ আপাততঃ বলবত্ অন্য কোন আইনে দোষী একই ব্যক্তির উপর অন্য কোন দণ্ড প্রদানে বাধা হইবে না৷

কতিপয় ক্ষেত্রে নেটওয়ার্ক সেবা প্রদানকারী দায়ী না হওয়া ৭৯৷ নেটওয়ার্ক সেবা প্রদানকারী কোন তৃতীয় পক্ষ তথ্য বা উপাত্ত প্রাপ্তিসাধ্য করিবার জন্য এই আইন বা তদধীন প্রণীত বিধি বা প্রবিধানের অধীন দায়ী হইবেন না, যদি প্রমাণ করা যায় যে, সংশ্লিষ্ট অপরাধ বা লংঘন তাহার অজ্ঞাতসারে ঘটিয়াছে বা উক্ত অপরাধ যাহাতে সংঘটিত না হয় তজ্জন্য তিনি সাধ্যমত চেষ্টা করিয়াছেন৷

ব্যাখ্যাঃ (ক) “নেটওয়ার্ক সেবা প্রদানকারী” অর্থ কোন যোগাযোগের মাধ্যম;

(খ) “তৃতীয় পক্ষ তথ্য বা উপাত্ত” অর্থ নেটওয়ার্ক সেবা প্রদানকারী কর্তৃক যোগাযোগের মাধ্যম হিসাবে যে তথ্য বা উপাত্ত প্রদান করা হয়৷

১১[ \*\*\*] আটক বা গ্রেফতারের ক্ষমতা ৮০৷ এই আইনের অধীন গৃহীত কোন অনুসন্ধান বা তদন্ত কার্যক্রমে নিয়ন্ত্রক, ক্ষমতাপ্রাপ্ত কোন কর্মকর্তা বা সাব-ইন্সপেক্টরের নিম্নে নহেন এমন কোন পুলিশ কর্মকর্তার যদি এইরূপ বিশ্বাস করিবার কারণ থাকে যে, কোন ১২[ \*\*\*] স্থানে এই আইনের পরিপন্থী কোন কার্য হইয়াছে বা হইতেছে অথবা এই আইনের অধীন দণ্ডণীয় কোন অপরাধ সংগঠিত হইয়াছে, তাহা হইলে অনুরূপ বিশ্বাস করিবার কারণ লিপিবদ্ধ করিয়া তিনি উক্ত স্থানে প্রবেশ করিয়া তল্লাশী করিতে পারিবেন এবং সংশ্লিষ্ট যে কোন বস্তু আটক করিতে পারিবেন এবং সংশ্লিষ্ট কোন ব্যক্তি বা অপরাধীকে গ্রেফতার করিতে পারিবেন৷

তল্লাশী, ইত্যাদির পদ্ধতি ৮১৷ এই আইনে ভিন্নরূপ কিছু না থাকিলে, এই আইনের অধীন জারীকৃত সকল তদন্ত, পরোয়ানা, তল্লাশী, গ্রেফতার ও আটকের বিষয়ে ফৌজদারী কার্যবিধির সংশ্লিষ্ট বিধানাবলী প্রযোজ্য হইবে৷

সাইবার আপীল ট্রাইব্যুনাল গঠন ৮২৷ (১) সরকার, সরকারী গেজেটে প্রজ্ঞাপন দ্বারা, এক বা একাধিক সাইবার আপীল ট্রাইব্যুনাল, অতঃপর সময় সময় আপীল ট্রাইব্যুনাল বলিয়া উল্লিখিত, গঠন করিতে পারিবে৷

(২) সাইবার আপীল ট্রাইব্যুনাল সরকার কর্তৃক নিযুক্ত একজন চেয়ারম্যান এবং দুইজন সদস্যের সমন্বয়ে গঠিত হইবে৷

(৩) চেয়ারম্যান এমন একজন ব্যক্তি হইবেন যিনি সুপ্রীমকোর্টের বিচারক ছিলেন বা আছেন বা অনুরূপ বিচারক হিসাবে নিয়োগ লাভের যোগ্য এবং সদস্যগণের মধ্যে একজন হইবেন বিচার কর্মবিভাগে নিযুক্ত একজন কর্মরত অথবা অবসরপ্রাপ্ত জেলা জজ এবং অন্য জন হইবেন তথ্য যোগাযোগ ও প্রযুক্তি বিষয়ে নির্ধারিত জ্ঞান ও অভিজ্ঞতা সম্পন্ন একজন ব্যক্তি৷

(৪) চেয়ারম্যান ও সদস্যগণ নিয়োগের তারিখ হইতে অন্যুন তিন বত্সর এবং অনধিক পাঁচ বত্সর পদে বহাল থাকিবেন এবং তাহাদের চাকুরীর শর্তাবলী সরকার কর্তৃক নির্ধারিত হইবে৷

সাইবার আপীল ট্রাইব্যুনালের এখতিয়ার ও পদ্ধতি ৮৩৷ (১) সাইবার ট্রাইব্যুনাল এবং, ক্ষেতমত, দায়রা আদালত কর্তৃক প্রদত্ত রায় ও আদেশের বিরুদ্ধে আপীল শ্রবণ ও নিষ্পত্তি করিবার এখতিয়ার আপীল ট্রাইব্যুনালের থাকিবে৷

(২) আপীল শ্রবণ ও নিষ্পত্তির ক্ষেত্রে, সাইবার আপীল ট্রাইব্যুনাল বিধি দ্বারা নির্ধারিত পদ্ধতি অনুসরণ করিবে এবং বিধি দ্বারা পদ্ধতি নির্ধারিত করা না হইলে সুপ্রীমকোর্টের হাইকোর্ট বিভাগ ফৌজদারী আপীল শুনানী ও নিষ্পত্তির জন্য যেইরূপ পদ্ধতি অনুসরণ করিয়া থাকে আপীল ট্রাইব্যুনাল সেইরূপ পদ্ধতি, প্রয়োজনীয় অভিযোজনসহ, অনুসরণ করিবে৷

(৩) সাইবার ট্রাইব্যুনাল কর্তৃক প্রদত্ত রায় বা আদেশ বহাল, বাতিল, পরিবর্তন, বা সংশোধন করিবার ক্ষমতা আপীল ট্রাইব্যুনালের থাকিবে৷

(৪) আপীল ট্রাইব্যুনাল কর্তৃক প্রদত্ত সিদ্ধান্ত চূড়ান্ত হইবে৷

সাইবার আপীল ট্রাইব্যুনাল গঠিত না হইবার ক্ষেত্রে আপীল পদ্ধতি ৮৪৷ এই অংশের অধীন কোন সাইবার আপীল ট্রাইব্যুনাল গঠিত না হইয়া থাকিলে, ফৌজদারী কার্যবিধি আইনে যাহা কিছুই থাকুক না কেন, দায়রা আদালত কিংবা, তেগত্রমত, সাইবার ট্রাইব্যুনাল কর্তৃক প্রদত্ত রায় ও আদেশের বিরুদ্ধে আপীল সুপ্রীমকোর্টের হাইকোর্ট বিভাগে দায়ের করিতে হইবে৷

This Act mainly deals-

ν Eliminates barriers to e-commerce,

ν Promotes legal and business infrastructures to secure e-transactions,

ν Facilitates electronic filing in government agencies and

ν Ensures efficient delivery of electronic records from government offices

ν Powers of Police Officers and Other Officers

ν Establishment of Cyber Appellate Tribunal.

Tribunal:

Tribunal shall conclude the trial within six months from the date of framingcharge. This period may be extended for three months. Tribunal shall pronounce its judgment within ten days after the conclusion of trial which may be deferred for tendays.

Cyber Appellate Tribunal:

The Government shall establish one or more cyber appellate tribunal. The appellate tribunal shall be constituted by one chairman and two member’s appointedby the Government. To be appointed as a chairman of Cyber Appellate Tribunal, hemust be either a former judge of the Supreme Court or existing judge of the Supreme Court or is eligible to be appointed as a judge of the Supreme Court.

One of the two members of the tribunal shall be a retired District Judge or employed in the judicial service and the other member must be an experienced and skilled person ininformation and communication technology. They shall be appointed for 3-5 years.

Cyber Appellate Tribunal shall have no original jurisdiction. It shall only hear and dispose of appeals from the order and judgment of the Cyber Tribunal and Sessions Court in appropriate cases.

The decision of the appellate tribunal shall befinal and it shall have the power to alter, amend, and annul the order and judgment of the cyber tribunal. The appellate tribunal shall follow the appellate procedure of High Court Davison of the Supreme Court. Until cyber appellate tribunal is established, appeal may be heard by the High Court Division.

Conclution:

Capacity of human mind is unfathomable. It is not possible to eliminate cyber crimefrom the cyber space. It is quite possible to check them. History is the witness that nolegislation has succeeded in totally eliminating crime from the globe. The onlypossible step is to make people aware of their rights and duties (to report crime as acollective duty towards the society) and further making the application of the lawsmore stringent to check crime. Undoubtedly the Act is a historical step in the cyberworld. Further I all together do not deny that there is a need to bring changes in theInformation Technology Act to make it more effective to combat cyber crime. I wouldconclude with a word of caution for the pro-legislation school that it should be kept inmind that the provisions of the cyber law are not made so stringent that it may retardthe growth of the industry and prove to be counter-productive.

Referrence

The Penal Code, 1860 (Act No. XLV of 1860) 2.

Mehta Dewang, Role of Police in Tackling Internet Crimes, 7.

The Information and Communication Technology Act, 2006.

Monjur Kader: Criminology (Cyber Crime) 11.

http://en.wikipedia.org/wiki/Cyber\_crime.

Duggal Pawan – The Internet: Legal Dimensions 8.