A brief study on notable provisions to tackle with Cyber Crime : Preventive and Judicial measures

Dr. Laba Thakuria[1]
Deputy Controller of Examination
AdtU

Pranab Kumar Goswami[2]
PhD scholar, Deptt. of Eng & Technology
AdtU

Abstract:

The paper highlights that, Cyber Crimes are such harmful activities in the cyberspace that cause huge damage not only to the individual but also to the person's property or even the society, state and the country. Being radically different from the conventional crimes, the law enforcement agencies also find it difficult to tackle cyber crimes because of inadequate knowledge about the computer systems. The menace of cyber crime criminality is not confined to one or two countries but the whole world is facing this gigantic problem as a 'technological scorn'. The technology has extended its tentacles cutting across national frontiers whereas the law is still struggling to define and redefine the boundaries for the control of cyber crimes. The cyber law particularly, the Information Technology Act,2000 is engaged in prevention and control of cyber crimes within the country's territorial jurisdiction overlooking the facts that cyber criminality is a global phenomenon which has no territorial limits.

1. INTRODUCTION:

Cyber security initiatives and projects in India are negligible in numbers. Even if some projects have been proposed, they have remained on papers only. Projects like National Cyber Coordination Centre (NCCC) of India, National Critical Information Infrastructure Protection Centre (NCIPC) of India etc failed to materialize so far. The National Cyber Security Policy of India 2013 also failed to take off and even if it is implemented it is weak on numerous aspects like privacy violation in general and civil liberties infringement in particular. It would not be wrong to say that India is a sitting duck in cyberspace and civil liberties protection regime.

Cyber security breaches are increasing world over and India is also facing this problem. The cyber security challenges before the Narendra Modi government would not be easy to manage as everything has to be managed from the beginning. There is a dire need to protect Indian cyberspace from sophisticated cyber-attacks. For instance, cyber security of critical infrastructures likes banks, automated power grids, satellites, thermal power plants, SCADA systems, etc. are vulnerable to cyber-attacks from around the world. The different acts and law are as follows

A. Information Technology Act, 2000 And Steps To Tackle The Cyber Crime:-

By passing the Information Technology Act, 2000 our Government has taken a great step forward to combat the menace of Cyber Crime. The Act has established the Cyber Regulations Appellate Tribunal having appellate jurisdiction. Being an appellate authority is entitled to exercise its appellate jurisdiction both on fact as also in law over a decision or order passed by the Controller of Certifying Authorities or the adjudication officer. Its power to examine the correctness, legality or property of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating officer is absolute.

The Act in Chapter 11, under Section 48-46 provides the establishment, powers and jurisdiction of the Cyber Regulation Appellate Tribunal. These Sections may be discussed as follows:-

i. Section 48: Establishment of Cyber Appellate Tribunal:-

a. The Central Government shall by notification, establish one more appellate tribunals to be known as the Cyber Regulation Appellate Tribunal.
b. The central government shall also specify, in the notification referred to in sub-section (1), the matters and places relation to which the

Cyber Appellate Tribunal may exercise jurisdiction.

ii. Section 49: Composition of Cyber Appellate Tribunal:-

Cyber Appellate Tribunal shall consist of one person only (here in after referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

iii. Section 50: Qualification for appointment as Presiding Officer of the Cyber Appellate Tribunal:-

A person shall not be qualified for appointment as Presiding Officers of a Cyber Appellate Tribunal unless he-

a. Is or has been or is qualified to be a judge of a High Court; or
b. Is or has been a member of the Indian Legal Service and is holding or has held a past in Grade I of that service for at least three years.

iv. Section 51: Terms of Office:-

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of 65 years whichever is earlier.

v. Section 52: Salary, allowances and other terms and conditions of service of Presiding Officer:-

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed.

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officers shall be varied to his disadvantage after appointment.

vi. Section 53: Filling up of vacancies:-

If for reason after than temporary absence, any vacancy in the office of the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

vii. Section 54: Resignation and removal:-

1. The Presiding Officer of a Cyber Appellate Tribunal may be notice in writing under his hand addressed to the Central Government, resign his office;

Provided that the said Presiding Officer shall, unless he is promised by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three 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 earlier.

2. The Presiding Officers 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 misbehaviour 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.

3. The Central Government may, by rules, regulation the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

viii. Section 55: Orders constituting Appellate Tribunal to be final and not invalidate its proceeding:-

No order of the Central Government appointing any person as the Presiding Officer 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.

ix. Section 56: Appeal to Cyber Appellate Tribunal:-

1. Save as provided in the Sub-Section (2), any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in this matter.

2. No appeal shall we to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

3. Every appeal under this Sub-section (1) shall be filled 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: Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of 45 days if it is satisfied that there has sufficient cause for not filling it within that period.

4. On receipt of an appeal under Sub Section (1),the Cyber Crime Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders there on as it thinks fit, confirming, modifying or setting aside the order appealed against.

5. The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal to the Concerned Controller or adjudicating officer.

6. The appeal field before the Cyber Appellate Tribunal under Sub-Section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within the six months from the date of receipt of the appeal.

x. Section 58: Procedure and Powers of the Cyber Appellate Tribunal:-

1. The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the Principal of natural justice and subject to the other provisions of this Act 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.

2. The Cyber Appellate tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely-

i. Summoning and enforcing the attendance of any person and examining him or both.
ii. Requiring the discovering and production of documents or other electronic records.
iii. Receiving evidence on affidavits.
Issuing commissions for the examination of witnesses or documents.
iv. Reviewing its decisions.
v. Dismissing an application for default or deciding it exparte.
vi. Any other matter which may be prescribed.

3. Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of Section 193 and 228, and for the purposes of Section 196 of the Indian Penal Code (45 of 1860) and the Cyber Appellate Tribunal shall deemed to be a Civil Court for the purposes of Section 195 and the Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

The Cyber Appellate Tribunal is a Civil Court. The Supreme Court in a Case of State of Maharashtra Vs. Marwanjee F. Desai, establishes the fact that the Tribunal is also a quasi-judicial authority. Supreme Court held that "Power of Authority to summon witnesses, enforce their attendance, examine them on oat or require discovery and production of documents show the quasi-judicial nature of proceedings before the authority."

xi. Power of Police Officer:

The Code of Criminal Procedure, 1973 gives to the police unfettered power to investigate all cases where they suspect that a cognizable offence has been committed. An "Investigation" means search for material and facts in order to find out whether or not an offences has been committed.

xii. Section- 78:- Power to investigate offences:

Notwithstanding anything committed in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Deputy Superintendent of Police shall investigate any offences under this Act.

xiii. Section 80:- Powers of Police Officer and other Officers to enter, search:

1. Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government

authorized by the Central Government in this behalf may enter any public place and search and arrest without any person found therein who is reasonably suspected to having committed or of committing or of being about to commit any offences under this Act.

2. Where any person is arrested under Sub-Section(1), by an officer other than a Police Officer, such officer shall, without unnecessary delay, take or send the person arrested before a Magistrate having jurisdiction in the case or before the Officer-in-Charge of a Police Station.

3. The provisions of Code of Criminal Procedure, 1973 (2 of 1974), shall subject to the provisions of this section, apply. So far as may be, in relation to any entry, search or arrest made under this section.

The provision was the most controversial at the time of passing the Information Technology Act. The opposition group described this provision as "draconian" and in "violation of human rights". Some of the politician stated that this provision is "misguided" and "downright dangerous". The Indian Police are not trained to detect cyber criminals, therefore, the approach ended that the provision could be used to here as the political opponents who use Internet for legitimate political activities.

This police station exclusively investigates Cyber Crime, such as- Computer Hacking, data damage, internet frauds, etc. The Cyber Crime Police Station (CCPS) is also going to set-up a website for receiving complaints from victims. Cyber Crime are of technical nature, therefore, the police need special training to deal with such cases. The Delhi Police have made compulsory for all new police constables and Sub-Inspectors to get Cyber Crime Investigation training. Two specialized centres have been setup at the police training for newcomers as well as for the officer already in service. The State of Tamilnadu has also launched three weeks capsule course on Cyber Crimes for Police Officers not below the rank of Deputy Superintendent to import investigating skill to control cyber-crimes.

The Cyber Crime Investigation Department (CID) in the State of Andhra Pradesh plans to setup a cyber-cell to deal with exclusively Cyber Crimes and on receipt of Government's permission it shall start functioning.

Getting the right lead and making the right interpretation are very important in solving a Cyber Crime. The Seven Stage continuum of a criminal case starts from perpetration, to registration to reporting, investigation, prosecution, adjudication and execution.

Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L, which the Kerela High Court has accepted through e-mail, Mr. T. K. Vishwanathan, has highlighted the requirement for introducing e-court in India. In his article published in The Hindu he has stated "If there is one area of Government where IT can make a huge difference to Indian Public is in the Judicial System." There has been many upcoming litigation in the field of Cyber Crime that has given a positive result and thereby sowing the seed of combating with Cyber Crime. In October, 2002 the Delhi High Court restricted a person from selling pirated Microsoft software over an Internet auction site.

B. PREVENTION OF CYBER CRIME:

Prevention is always better than cure. It is always better to take certain precaution while working on the Internet. Sailash Kumar Zarkar, Technical Advisor and Norton Security Consultant to the Mumbai Police Cyber Crime Cell, advocate the 5 mantra for online security: Precaution, Prevention, Protection and Perseverance. The best way to combat all the ever increasing C.C is to sensitize and spread awareness among the wide spread users of the cyber space.[17]

Cybercrime prevention can be straight-forward - when armed with a little technical advice and common sense, many attacks can be avoided. In general, online criminals are trying to make their money as quickly and easily as possible. The more difficult you make their job, the more likely they are to leave you alone and move on to an easier target. The tips below provide basic

information on how you can prevent online fraud.

i. Keep your computer current with the latest patches and updates.

One of the best ways to keep attackers away from your computer is to apply patches and other software fixes when they become available. By regularly updating your computer, you block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into your system.

While keeping your computer up-to-date will not protect you from all attacks, it makes it much more difficult for hackers to gain access to your system, blocks many basic and automated attacks completely, and might be enough to discourage a less-determined attacker to look for a more vulnerable computer elsewhere.

More recent versions of Microsoft Windows and other popular software can be configured to download and apply updates automatically so that you do not have to remember to check for the latest software. Taking advantage of "auto-update" features in your software is a great start toward keeping yourself safe online.

ii. **Make sure your computer is configured securely.**

Keep in mind that a newly purchased computer may not have the right level of security for you. When you are installing your computer at home, pay attention not just to making your new system function, but also focus on making it work securely.

Configuring popular Internet applications such as your Web browser and email software is one of the most important areas to focus on. For example, settings in your Web browser such as Internet Explorer or Firefox will determine what happens when you visit Web sites on the Internet—the strongest security settings will give you the most control over what happens online but may also frustrate some people with a large number of questions ("This may not be safe, are you sure you want do this?") or the inability to do what they want to do.

Choosing the right level of security and privacy depends on the individual using the computer. Oftentimes security and privacy settings can be properly configured without any sort of special expertise by simply using the "Help" feature of your software or reading the vendor's Web site. If you are uncomfortable configuring it yourself consult someone you know and trust for assistance or contact the vendor directly.

iii. **Choose strong passwords and keep them safe.**

Passwords are a fact of life on the Internet today—we use them for everything from ordering flowers and online banking to logging into our favourite airline web site to see how many miles we have accumulated. The following tips can help make your online experiences secure:

- Selecting a password that cannot be easily guessed is the first step toward keeping passwords secure and away from the wrong hands. Strong passwords have eight characters or more and use a combination of letters, numbers and symbols (e.g., # $ % ! ?). Avoid using any of the following as your password: your login name, anything based on your personal information such as your last name, and words that can be found in the dictionary. Try to select especially strong, unique passwords for protecting activities like online banking.

iv. **Protect your computer with security software.**

Several types of security software are necessary for basic online security. Security software essentials include firewall and antivirus programs. A firewall is usually your computer's first line of defence-it controls who and what can communicate with your computer online. The next line of defence many times is your antivirus software, which monitors all online activities such as email messages and Web browsing and protects an individual from viruses, worms, Trojan horse and other types malicious programs.

v. Protect your personal information.

Exercise caution when sharing personal information such as your name, home address, phone number, and email address online. To take advantage of many online services, you will inevitably have to provide personal information

in order to handle billing and shipping of purchased goods. Since not divulging any personal information is rarely possible, the following list contains some advice for how to share personal information safely online:

- **Keep an eye out for phony email messages**.

Things that indicate a message may be fraudulent are misspellings, poor grammar, odd phrasings, Web site addresses with strange extensions, Web site addresses that are entirely numbers where there are normally words, and anything else out of the ordinary. Additionally, phishing messages will often tell you that you have to act quickly to keep your account open, update your security, or urge you to provide information immediately or else something bad will happen. Don't take the bait.

- **Don't respond to email messages that ask for personal information.**

Legitimate companies will not use email messages to ask for your personal information. When in doubt, contact the company by phone or by typing in the company Web address into your Web browser.

- **Steer clear of fraudulent Web sites used to steal personal information.**

When visiting a Web site, type the address (URL) directly into the Web browser rather than following a link within an email or instant message. Fraudsters often forge these links to make them look convincing.

- **Pay attention to privacy policies on Web sites and in software.** It is important to understand how an organization might collect and use your personal information before you share it with them.

- **Guard your email address.**

Spammers and phishers sometimes send millions of messages to email addresses that may or may not exist in hopes of finding a potential victim. Responding to these messages or even downloading images ensures you will be added to their lists for more of the same messages in the future.

vi. **Online offers that look too good to be true usually are.**

The old saying "there's no such thing as a free lunch" still rings true today. Supposedly "free" software such as screen savers or smileys, secret investment tricks sure to make you untold fortunes, and contests that you've surprisingly won without entering are the enticing hooks used by companies to grab your attention.

While you may not directly pay for the software or service with money, the free software or service you asked for may have been bundled with advertising software ("adware") that tracks your behavior and displays unwanted advertisements. You may have to divulge personal information or purchase something else in order to claim your supposed content winnings.

vii. **Review bank and credit card statements regularly.**

The impact of identity theft and online crimes can be greatly reduced if you can catch it shortly after your data is stolen or when the first use of your information is attempted. One of the easiest ways to get the tip-off that something has gone wrong is by reviewing the monthly statements provided by your bank and credit card companies for anything out of the ordinary.

Additionally, many banks and services use fraud prevention systems that call out unusual purchasing behavior (i.e. if you live in Texas and all of the sudden start buying refrigerators in Budapest). In order to confirm these out of the ordinary purchases, they might call you and ask you to confirm them..

C. CONCLUSION:

All the nations should therefore, realize the need and urgency for generating awareness about the dangerous nature of cyber crimes which are perpetuating illegal online activities in cyberspace. Cyber criminality is perhaps the deadliest epidemic spread over the world, which has to be curbed by adoptive global preventive strategy.

The ultimate solution in this regard is to formulate a techno legal framework that can

safeguard Indian cyberspace in the best possible manner. A dedicated cyber security law of India and implementable cyber crisis management plan is also required. Outdated and draconian laws like cyber law and telegraph Act of India must also be repealed immediately.

In these circumstances cyber security needs urgent attention of Indian government. In a positive development, the National Cyber Coordination Centre (NCCC) of India may finally see the light of the day and may become functional very soon. The NCCC would help India is fighting against national and international cyber threats. Very soon it would be clear how far the BJP government would go to protect Indian cyberspace.

Police has a special responsibility to prevent youngsters indulging in Cyber Crime and also to ensure that Cyber Cafe should not become crime hubs. It is an arduous task to control the illegal activities of criminals having high-tech experience. In order to handle cyber-crimes, like other countries, India's first cyber police station was set up in Bangalore city and that started functioning in September, 2001.

A nationwide survey of cyber law indicates that only a few countries have updated their cyber law to counter the cyberspace crime effectively, while many countries have note even initiated steps to frame laws for policing against these crimes. This divergent approach of world nation towards the desirability of cyber law possesses a real problem in handling the internet crime and at the same time provides ample scope for the cyber criminals to escape detention and punishment.

D. REFERENCES:

1. Information Technology, Law and Practice, Universal Law Publishing, 3rd Edition, Vakul Sharma.

2. Cyber defamation in india (law on internet), New Era publication, 4th edition, Dr farooq Ahmed

3. Information Technology, Law & Practice, Universal Law Publication, 3rd Edition, Vakul Sharma.

Websites :

1. https://en.wikipedia.org/wiki/terrorism

2. https://en.wikipedia.org/wiki/Cyberspace

3. www.cyberforensics.com

4. Https://www legalcrystal.com

5. www.helpline.com/govt/cyber defamation in india.

6. www.mylegaladvisor.in/blog-mla/cyber defamation