Cyber Laws in India: An Overview

***Dr. Sonia Dutt Sharma, Associate Professor**

**** Prashant Kumar, Research Scholar, MJRP, University, Jaipur, Rajasthan.**

Abstract

Fast growing internet has its own advantages as well as disadvantages. The increasing use of information technology facilitate common people to get information, store information, share information etc. Internet provides great facilities to society but same time it present opportunities for crime also. Credit card frauds, spams, defamation or hate expression on the social networking sites and piracies are some of disadvantages due to illegal activities on internet. Cyber Law has emerged due to proliferation of misuse of the computer and internet in the cyber space. The content of this article is intended to provide a general guide to the subject matter.

In present paper there is brief discussion about cyber law and cyber crime and legal provisions to overcome cyber crimes and penalty there for.

Key Words: ***Cyber Crime, I.T. Act, Internet, Computer etc***.

Introduction

Computer and internet becomes very common and necessary for the daily life of the present generation. Now approximately *250 Crore* people are hooked up to surf the internet around the globe by virtue of increasing facilities in the mobile phones, tabs, and laptops etc.. By internet, www and online service and activities users can access data anytime and from any place. This includes not only educational and informative material but also information that might be personal. The present time of fast computing brings a new world known as cyber world. The increasing use of information technology facilitate common people to get information, store information, share information etc. The cyber world is an online world where users have a lot of information technology mechanisms to do personal activity as easily and freely as they can transact them in the physical world.

Due to massive increase in the use of Internet and dependency of individuals on it in every field, a number of new crimes related to Computer and other gadgets based on internet have evolved in the society. Such crimes where use of computers coupled with the use of Internet is involved are broadly termed as Cyber Crimes.

Cyber Crime: As the use of internet is increasing, a new face of crime is spreading rapidly from in-person crime to nameless and faceless crimes involving computers. Cyber crime includes all unauthorized access of information and break security like privacy, password, etc. with the use of internet. Cyber crimes also includes criminal activities performed by the use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system, etc. There are two ways of cyber crime; computer as weapon, and computer as target. In first way computer is used to harm others property by use of internet or hacking id, while in other the attacker targets to harm or destroy computer.

In tenth United Nations congress on “prevention of crime and treatment of offenders” which is devoted to issues of crimes related to computer networks, cyber crime was broken into two categories and defined as:

***a. Cyber crime in a narrow sense (computer crime*):** Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cyber crime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Facets of Cyber Crime

Following are the few examples of cyber crime:

Cyber stalking: Online harassment and online abuse all comes under stalking. It generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Cyber stalking shares important characteristics with offline stalking; many stalkers (online or off) are motivated by a desire to control their victims. A major damaging effect of online abuse is a victim avoiding his/her friends, family and social activities.

Intellectual Property Crimes: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially, of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

Bot Networks: The word botnet made from the two words robot and network. A cyber crime called 'Bot Networks', when hackers remotely take control upon computers by using malware software. Computers can be co-opted into a botnet when they execute malicious software. A botnet's originator can control the group remotely.

Transmitting Virus: Viruses are programs that attach themselves to a computer or a file, and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it.

Worm attacks plays major role in affecting the computerize system of the individuals.

Hacking: In general words hacking means seeking and exploiting weakness and security of a computer system or a computer network for unauthorized access. The person who does hacking is known as hacker. Hacker use computer expertise and some tool or scripts to hack any computer system.

Internet Time Thefts: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else’s ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person’s knowledge.

Cracking: It is a dreadful feeling to know that a stranger has broken into user computer systems without user’s knowledge and consent and has tampered with precious confidential data and information. Cracker are differ with hacker because hacker are hired by

companies to audit network security or test software but cracker do same work for their own profit or to harm others.

Phishing: Phishing means acquire information such as usernames, passwords, credit card details, personal detail etc by electronic communication. Phishing commonly uses fake emails or fake messages which contain link of virus/ malware infected fake websites. These websites request user to enter their personal detail.

Voice Phishing: The term is a combination of "voice" and phishing. Voice phishing is use to gain access of private, personal and financial information from the public. Voice phishing uses a landline telephone call to get information.

Monetary Benefits: Monetary benefits are getting benefits through withdrawing money by hacking the victim's bank account.

E-Mail/SMS Spoofing: A spoofed E-mail/ SMS may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates. Here an offender steals identity of another in the form of email address, mobile phone number etc and send message via internet.

Cross-site Scripting: Cross-site scripting (XSS) is a type of computer security vulnerability. By cross-site scripting attacker can bypass the predefine access permissions of website. Reflected XSS is the most frequent type of XSS attack. Reflected XSS attack is also known as non-persistent XSS. Scripting languages like java script, VBScript etc are use for Reflected XSS attack.

Cyber Squatting: Squatting is the act of occupying an abandoned or unoccupied space. Cyber squatting is the act of registering a famous domain name and then selling it to needy in high cost. It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.

Child Pornography: It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. Child pornography is divided into *simulated child pornography* and *pornography* which was produced with direct involvement of the child (also known as child abuse images).

Cyber Vandalism: Vandalism means destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person.

Cyber Trespass: It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

Cyber Trafficking: It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.

Cyber crime & Social Networking: Cyber criminals use social media not only to commit crime online, but also for carrying out real world crime owing to "over-sharing" across these social platforms**.** The risk associated with our identities. Identity theft can happen to anyone who exposes too much personal information online on various social networking sites. Get to know the security and privacy settings, and configure them to protect from identity theft. One in five online adults (21 percent) has reported of becoming a victim

of either social or mobile cyber crime and 39 percent of social network users have been victims of profile hacking, scam or fake link.

Laws Governing to Cyber Crimes in India

There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology "INFORMATION TECHNOLOGY ACT, 2000" [ITA- 2000] was enacted by Parliament of India, having 94 Sections and 2 Schedules to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes. The above Act was further amended in the form of IT Amendment Act, 2008 [ITAA-2008].

Cyber law was first step taken by Government to overcome cybercrime. According to Indian law cyber crime has to be voluntary and wilful, an act or omission that adversely affects a person or property. Cyber law encompasses laws relating to Cyber Crimes, Electronic and Digital Signatures, Intellectual Property, Data Protection and Privacy. Indian parliament passed its first "*Information Technology Act, 2000*" on 17th October 2000 to deal with cybercrime in the field of e-commerce, e-governance, embanking as well as penalties and punishments. The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable.

On 17th October 2000 the Information Technology (Certifying Authorities) Rules, 2000 and Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 came into force. On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. (Security Procedure) Rules, 2004 came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. An important order relating to blocking of websites was passed on 27th February, 2003. According to which, Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website.

Despite of I. T. Act, the Indian Penal Code (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc. Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act). In case of bank records, the provisions of the Bankers' Book Evidence Act (as amended by the IT Act) are relevant. Investigation and adjudication of cyber crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act. The Reserve Bank of India Act was also amended by the IT Act.

The ***I.T. Act, 2000*** defines under ***Section 2 (i)***'computer' means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, 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. The word 'computer' and 'computer system' have been so widely defined and interpreted to mean any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities and therefore any high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition.

Scope and applicability

The scope and applicability of ITA-2000 was increased by its amendment in 2008. The word 'communication devices' inserted having an inclusive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc like what was later being marketed as iPod or other similar devices on Wi-fi and cellular models. Though I.T. Act, 2000 defined 'digital signature' in ***Section 2 (p)***, however said definition was incapable to cater needs of hour and therefore the term 'Electronic signature' was introduced and defined in the I.T. Act, 2008 as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone.

The new amendment has replaced ***Section 43*** with ***Section 66***. The Word "hacking" used in ***Section 66*** of earlier Act has been removed and named as "data theft" in this section and has further been widened in the form of ***Sections 66A to 66F***. The section covers the offences such as the sending of offensive messages through communication service, misleading the recipient of the origin of such messages, dishonestly receiving stolen computers or other communication device, stealing electronic signature or identity such as using another persons' password or electronic signature, cheating by personation through computer resource or a communication device, publicly publishing the information about any person's location without prior permission or consent, cyber terrorism, the acts of access to a commuter resource without authorization, such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus like Trojan etc. The offences covered under ***Section 66*** are cognizable and non-bailable. Whereas, the consequence of ***Section 43*** of earlier Act were Civil in nature having its remedy in the form of damages and compensation only, but under ***Section 66*** of the Amendment Act, if such act is done with criminal intention that is *mens rea*, then it will attract criminal liability having remedy in imprisonment or fine or both.

Adjudication: Adjudication powers and procedures have been dealt in **Sections 46** and thereafter. As per the Act, the Central Government may appoint any officer not below the rank of a director to the Government of India or a state Government as the adjudicator. The I.T. Secretary in any state is normally the nominated Adjudicator for all civil offences arising out of data thefts and resultant losses in the particular state. Very few applications were received during first 10 years of existence of the I.T. Act, that too in the major metros only. However, the trend of receiving complaint under I.T. Act is rapidly growing. The first adjudication obtained under this provision was in Chennai, Tamil Nadu, in a case involving ICICI Bank in which the bank was told to compensate the applicant with the amount wrongfully debited in Internet Banking, along with cost and damages. There is an appellate procedure under this process and the composition of Cyber Appellate Tribunal at the national

level, has also been described in the Act. Every adjudicating officer has the powers of a civil court and the Cyber Appellate Tribunal has the powers vested in a civil court under the Code of Civil Procedure.

The major Acts, which got amended after enactment of I.T. Act: The I.T. Act brought a wide change in the Indian legal system. The major Acts, which got amended after enactment of I.T. Act are following:

The Indian Penal Code, 1860

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. ***Sections 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc***) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/ charge sheet quoting the relevant sections from IPC under ***Section 463,464, 468 and 469*** read with the I.T. Act / I.T. Amendment Act under ***Sections 43 and 66*** in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.

The Indian Evidence Act 1872

Prior to enactment of I.T. Act, all evidences in a court were in the physical form only. After existence of I.T. Act, the electronic records and documents were recognized. The definition part of Indian Evidence Act was amended as "all documents including electronic records" were substituted. Other words e.g. 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the I.T. Act, were also inserted to make them part of the evidentiary importance under the Act. The important amendment was seen by recognition of admissibility of electronic records as evidence as enshrined in ***Section 65B*** of the Act.

The Bankers' Books Evidence (BBE) Act 1891*:*

Before passing of I.T. Act, a bank was supposed to produce the original ledger or other physical register or document during evidence before a Court. After enactment of I.T. Act, the definitions part of the BBE Act stood amended as: "'bankers ' books' include ledgers, day-books, cashbooks, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc, a printout of such entry ...certified in accordance with the provisions ....to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data ...to retrieve data that is lost due to systemic failure or ....

The above amendment in the provisions in Bankers Books Evidence Act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided, such print-out or electronic document is accompanied by a certificate in terms as mentioned above.

Issues not covered under I.T. Act

I.T. Act and I.T. Amendment Act is though landmark first step and became mile-stone in the technological growth of the nation; however the existing law is not sufficed. Many issues in Cyber crime and many crimes are still left uncovered.

Territorial Jurisdiction is a major issue which is not satisfactorily addressed in the I.T. Act or I.T. Amendment Act. Jurisdiction has been mentioned in ***Sections 46, 48, 57 and 61*** in the context of adjudication process and the appellate procedure connected with, and again in ***Section 80***, and as part of the police officers' powers to enter, search a public place for a cyber crime etc. Since cyber crimes are basically computer based crimes and therefore if the mail of someone is hacked in one place by accused sitting far in another state, determination of concerned Police Station, who will take cognizance is difficult. It is seen that the investigators generally try to avoid accepting such complaints on the grounds of jurisdiction. Since the cyber crime is geography-agnostic, borderless, territory-free and generally spread over territories of several jurisdiction; it is needed to proper training is to be given to all concerned players in the field. Preservation of evidence is also big issue. It is obvious that while filing cases under I.T. Act, very often, chances to destroy the necessary easily as evidences may lie in some system like the intermediaries' computers or sometimes in the opponent's computer system too. However, most of the cyber crimes in the nation are still brought under the relevant sections of IPC read with the comparative sections of I.T. Act or the I.T. Amendment Act which gives a comfort factor to the investigating agencies that even if the I.T. Act part of the case is lost, the accused cannot escape from the IPC part.

Penalty for Damage to Computer System

According to the ***Section 43*** of the **'Information Technology Act, 2000'** whoever does any act of destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be punishable. According to the ***Section 43A*** which is inserted by the **'Information Technology(Amendment) Act, 2008'** where a body corporate is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. Section 66 deals with 'computer related offences' and provides for imprisonment up to 3 years or fine, which may extend up to 5 lakh rupees or both.

Best Practices for Prevention of Cyber Crime

Below mentioned security guidelines and good practices may be followed to minimize the security risk of Cyber crime:

By updating the computer: To avoid cyber attacks, regularly update operating system of computers and antivirus. While keeping computer up to date will not protect user from all attacks, it makes it much more difficult for hackers to access computer system, blocks many basic and automated attacks completely etc.

By choosing strong passwords (Alfa numeric): Passwords are online identity over internet. Always select a password that have at least eight characters and use a combination of letters, numbers, and symbols (e.g. # $ % ! ?). Avoid using easy password like name, city name etc.

use non dictionary words. Keep passwords in safe place and not use same password for every online service. Change passwords on a regular basis, at least every 90 days.

By protecting computer with security software: Security software commonly includes firewall and antivirus programs. A firewall controls who and what can communicate with computer online. Antivirus software monitors all online activities and protects computer from viruses, worms, Trojan horses, and other types of malicious programs. Antivirus and antispyware software should be configured to update itself, and it should do so every time connect to the Internet.

Shield personal information: To take advantage of many online services, users will have to provide personal information in order to handle billing and shipping of purchased goods. The following list contains some advice for how to share personal information safely online:

- Phishing messages will often tell that to act quickly to keep account open, update security, or else something bad will happen. Don't respond them.
- Don't respond to email messages that ask for personal information. True companies will not use email messages to ask for personal information.
- When visiting a website, type the URL directly into the Web browser rather than follow a link within an email or instant message.
- Guard email address from unwanted emails.

Online offers that look too good to be true usually are: The free software or service asked for may have been bundled with advertising stuff that tracks behaviour and displays unwanted advertisements. Be careful while downloading free stuff.

Review bank and credit card statements regularly: The impact of identity theft and online crimes can be greatly reduced if user can catch it shortly after their data is stolen or when user gets symptoms. Regularly check bank and credit card's statements. Now, many banks and services use fraud prevention systems that call out unusual purchasing behaviour.

Be Social-Media knowledge: Make sure social networking profiles (e.g. Facebook, Twitter, etc.) are set to private. Check security settings with in frequent intervals. Be careful what information post online.

Secure Mobile Devices: Be aware that mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

Secure wireless network: Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Avoid using public WiFi spots.

Call the right person for help: If computer crime is suspected by a way of identity theft or a commercial scam then immediately report this to local police. If help is needed for maintenance or software installations on computer then consult with authenticated service provider or a certified computer technician.

Cyber Crime Cells in India

To solve cyber crime cases, Indian police developed cyber crime investigation cells all over India(Assam, Bangalore, Bihar, Chennai, Delhi, Gujarat, Haryana, Himachal Pradesh, Hyderabad, Jammu, Jharkhand, Kerala, Meghalaya, Mumbai, Orissa, Pune, Punjab, Thane, Uttar Pradesh, Uttarakhand, West Bengal etc.). These Cyber Crime cell investigates in respect of cases pertaining to hacking, spread of virus, pornography, manipulation of accounts, alteration of data, software piracy, creation of false Web sites, printing of

counterfeit currency, forged visas, theft of intellectual property, email spamming, denial of access, password theft, crimes with cell phones and palmtops, cyber terrorism etc..

Conclusion

Society as on today is happening more and more dependent upon cyber technology and consequently crime based on electronic offences are bound to increase. At present criminals have changed their method and have started using advanced technology. In order to deal with them the society, the legal and law enforcement authorities will also have to change. All cyber crime is based on lack of awareness. This is a duty of Government, print media to educate unwary persons about the dangerous areas of the cyber-world because prevention is better than cure. Cyber Space Security Management has already become an important component of National Security Management, Military Security Management, Scientific Security Management and Intelligence Management all over the world. Endeavour of law making machinery of the nation should be in accordance with mile compared to the fraudsters, to keep the crimes lowest. Hence, it should be the persistent efforts of rulers and law makers to ensure that governing laws of cyber technology contains every aspect and issues of cyber crime and further grow in continuous and healthy manner to keep constant vigil and check over the related crimes.

.

References

- "*The Information Technology Act, 2000*" (as amended by I. T. Act, 2008).
- Sharma Vakul, *"Information Technology Law and Practice"*, 3rd ed. 2011, Universal Law Pub., New Delhi.
- Vishwanathan Aparna, "*Cyber Law: Indian and International Perspective*",LexisNexis Butterworth Wadhwa pub. Nagpur, 2012.
- Singh Talwant, Additional District & Sessions Judge, New Delhi, India, "*Cyber Law & Information Technology*" (2011).
- Nagpal Rohas, "*Introduction to Indian Cyber Law*" (2008), Asian School of Cyber Laws, Pune, India.
- Suri R.K. and Chhabra T.N., "*Cyber Crime*" (2003), Pentagon Press, New Delhi, India.
- Seth Karnika "*Cyber Laws in the Information Technology Age*" (2009), Jain Book Depot, New Delhi, India.
- http://www.philstar.com/business/2013/03/12/918801/study-social-networks-new-haven-cybercrime.
- http://www.symantec.com/en/in/about/news/release/article.jsp?prid=20130428_01
- http://www.internetworldstats.com/stats.htm.
- http://en.wikipedia.org/wiki/Computer_crime.