CYBER CRIMES AND ITS RELATED LAWS

Vanita Bansal[1]

Since the Beginning of civilization, man has always been motivated by the need to make progress and improve the existing technologies. This lead to tremendous development and progress. One of the most significant development made by mankind is the development of Internet. Internet has emerged as a blessing for the present pace of life. It made life easier in e-banking, business networking, economic affairs etc.

Due to immense increase in the use of Internet and dependency of individuals in every field, a number of new crimes related to computer and other gadgets based on Internet have emerged in society. Internet resulted in various threats to the consumers and other institutions inspite of the fact of being beneficiary to them. Such crimes where use of computers coupled with the use of Internet is involved are broadly termed as CYBER CRIMES. Various criminals like hackers, crackers have been able to pave their way to interfere with the Internet accounts through various techniques like hacking Domain Name Server (DNS), Internet Provider's (IP) address, spoofing, phishing etc. They succeed in gaining access to user's computer system.

Cyber Crime is an international problem with no national boundaries. Hacking attack can be launched from any corner of the world without any fear of being traced. Cyber terrorists can collapse the economic structure of a country from anywhere. These types of crimes can only be combatted by technology but there is always a threat that hackers can misuse it by their

[1]Advocate, Kurukshetra, Haryana, India.

techniques. Countries throughout the world are resorting to different approaches towards controlling, regulating and facilitating electronic communication and commerce.

TYPES OF CYBER CRIMES

Cyber terrorists use the computer as a tool, target and for their unlawful act to gain information which can result in heavy loss/damage to the owner. By Internet, offenders can gain any information of companies, firms, individuals, and banks, sell illegal articles, pornography etc. Many banks, financial institutions, investments houses etc. are being threatened by the cyber terrorists to pay extortion money to keep their sensitive, information intact to avoid huge damages. Cyber Crimes can be basically divided into three major categories:

- Cybercrimes against persons - Cyber Crime against persons includes various crimes like transmission of child- pornography, harassment of any one with the use of computer and cyber stalking.
- Cybercrimes against property - Cyber Crime against property includes unauthorized computer trespassing through cyberspace, computer vandalism, and transmission of harmful program.
- Cybercrimes against Government - Cyber Crime against Government is Cyber terrorism. Individuals and groups to threaten international Government to terrorize the citizens are using the medium of cyber space.

LAW TO TACKLE THE PROBLEM OF CYBER CRIME

The Parliament has passed its first Cyber law, THE INFORMATION TECHNOLOGY ACT 2000 that provides legal infrastructure for e- commerce in India. Cyber law is important because it touches almost all aspects of transactions and activities involving the Internet, WWW, and cyber space. The Standing Committee made several suggestions but the most important was that a cyber café owner must maintain a register to record the manes and address

of all people visiting his café and also a list of websites they surfed. It was made as an attempt to curb cybercrime and to facilitate speedy locating of a cybercriminal. But this suggestion invades upon a net surfers' privacy and dropped by IT Ministry.

The Act had been amended in 2008 to increase its scope. The word 'Communication devices' inserted as including cell phones, personal digital assistance or other devices used to transmit text, videos etc. New concept of 'electronic signature' was introduced and defined as a legally valid mode of executing signatures. Inserting the word 'electronic' thereby treating the electronic records and documents on par with physical records and documents amended the IPC. The sections dealing with false entry in a record or false document etc. have been amended as 'electronic record and electronic document'. Prior to enactment of ITA, all evidences in a court were in the physical from only. After existence of ITA, the electronic records and documents were recognized. The definition part of Indian Evidence Act was amended as 'all documents including electronic records' were substituted.

ITA 2000 is India's nodal legislation regulating the use of computers, computer systems, and computer networks. It had touched varied aspects pertaining to electronic authentication, digital signatures, cybercrimes and liability of network service providers. It aims at providing legal recognition for transactions carried out by means of electronic data and other means of electronic communication referred as 'e- commerce'.

PROVISIONS OF INFORMATION TECHNOLOGY ACT 2008

Section 2[2] deals with digital signatures and electronic signatures. Any subscriber can authenticate an electronic record by affixing his digital signature and electronic signature. Section 3[3] provides recognition to electronic records and Section 5[4] provides legal recognition to electronic signatures. Section 6[5] says for the use e-records and e- signatures in Government and its agencies in a particular manner prescribed by appropriate Government. Another provision of Information Technology Act says that the Government may authorize any service provider to set up, maintain and upgrade computerized facilities. Section 10A[6] deals with

---

[2] Section 2 (d) "Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature; Section 2 (p) "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

[3] Section 3 of Information Technology Act - Any subscriber may authenticate an electronic record By affixing his Digital Signature.

[4] Section 5 of Information Technology Act- Legal recognition of Electronic Signature Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

[5] Section 6 of Information Technology Act – Use of Electronic Records and Electronic Signature in Government and its agencies (1) Where any law provides for

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

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

(c) the receipt or payment of money in a particular manner, then, notwithstanding

Anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

[6] Section 10A talks about the Validity of contracts formed through electronic means (Inserted by ITAA 2008)

validity of contracts formed through electronic means. All proposals, acceptance, revocation etc. are expressed in electronic form. Section 7[7] stipulates the principle of law for retention of electronic records in those cases where the existing laws do not expressly provide for the retention of documents, records or information in the form of e-records. Section 8[8] provides for the publication of the official Gazette in the e-form referred as e-gazette. Section 10[9] gives the Central Government the power of discretion to prescribe various rules in respect of digital

---

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

[7] Section 7 of Information Technology Act - Retention of Electronic Records says that where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.

[8] Section 8 of Information Technology Act says that Publication of rules, regulation, etc, in Electronic Gazette Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

[9] Section 10 of Information says that The Central Government may, for the purposes of this Act, by rules, prescribe (a) the type of Electronic Signature;

(b) the manner and format in which the Electronic Signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the Electronic Signature;

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

(e) any other matter which is necessary to give legal effect to Electronic Signature.

signatures. Section 64[10] outlines the procedure for recovery of penalty imposed. If the said penalty is not paid, it shall be recovered as an arrear of land revenue. Another provisions of Information Technology Act, 2008 provides compensation for any damage to the computer systems etc. If any person without permission of the owner access the computer system, downloads, copies any data or other information, causes any computer virus, steals, conceals, destroys or alters any information shall be punished. If a body corporate, possessing, dealing or handling any sensitive personal data or information fails to do so or do negligent act, he shall be liable to pay damages of Rs. 5 crore to the person affected. Section 44[11] says if any person is required to give information, return or report to the Controller or the Certifying Authority fails to furnish the same, shall be liable to a penalty of Rs. One lakh and Rs. 50,000 for each failure. Under Section 46[12] the Central Government or State Government may appoint adjudicating officers to deal with cybercrimes. Government also establish Cyber Appellate Tribunals to deals with the appeals. This Tribunals consists of a chairperson and such number

---

[10] Section 64 of Information Technology Act says that a penalty imposed or compensation awarded under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the license or the Electronic Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

[11] Section 44 of Information Technology Act talks about Penalty for failure to furnish information, return, etc
If any person who is required under this Act or any rules or regulations made thereunder to -
(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:
(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

[12] Section 46 of Information Technology Act - the Central Government shall, subject to the provisions of sub-section(3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

of other members, as the Central Government may appoint. Chairperson shall have the powers of general superintendence.

OFFENCES UNDER INFORMATION TECHNOLOGY ACT AND THEIR PENALITIES

Section 65[13] is the provision that specifies various kinds of cybercrimes, which have been made penal offences punishable with imprisonment or fine or both. Tempering with computer source code used for computer, computer program, computer system or computer network is a penal offence. For this punishment of imprisonment of three years and Rs. 2 lakh fine prescribed.

In **State of UP V. Saket Songhai's,**[14] The Police registered a case against Saket Singhania for making alterations in the SIMPL Program to sell it. Section 66[15] defines the offence of hacking. It means an act of intruding into someone's computer without his knowledge or consent. Punishment prescribed is fine of Rs. Two lakhs and three years' imprisonment. In **Delhi vidyut Board Case[16],** hacking was found. The IITian worked out the system in such a way that he siphoned money and transferred it to his personal account. The typical case of hacking emerged in Raigarh, Chattisgarh which was reported in the media investigations revealed the modus operandi of the cybercrime. This happened where the sender of the mail kept a file in a directory

---

[13] Section 65 of Information Technology Act -Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

[14] State of UP V. Saket Songhai's

[15] Section 66 of Information Technology Act - If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

[16] Abul Hassan And National Legal V. Delhi Vidyut Board & Ors. 1999 IIAD Delhi 105, AIR 1999 Delhi 88, 77 (1999) DLT 640, 1999 (48) DRJ 483

named Akshdoot.Doc. Investigations revealed that Akshdoot was a project like Gyandoot of Dhar and run by Aptech Computer Education Raigarh. Police raided Aptech Center and found all sent mails and the files. In **CK KARODKAR V. STATE OF MAHARASTRA[17]:** Supreme Court held that the standards of obscenity would differ from country to country depending on the standards of morals. It is the duty of the court to consider the obscene matter by taking an overall passages. In **STATE OF TAMILNADU V. D.L. PRAKASH[18]:** The case assumes tremendous importance in the light of fact that online pornographic and brokers have been targeted for the first time in our country. Accessing or viewing any pornographic or obscene electronic information has not been made a penal offence.

Various tests were laid down in course of time to determine the actual crime in case of obscene material published in electronic form on net. HICKLIN test was adopted in America. In case of **Regina V. Hicklin**[19] Where it was held," if the material has tendency is to deprive and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall". In Indian Scenario the case of **Ranjeet d. Udeshi V. State of Maharastra[20],** the Supreme Court admitted that IPC doesn't define obscenity though it provides punishment for publication of obscene matter.

According to Section 68[21], any certifying authority who fails to comply with any order of Controller shall be guilty of an offence and liable to imprisonment for a term not exceeding

---

[17] Chandrakant Kalyandas Kakodar vs The State Of Maharashtra And Ors 1970 AIR 1390, 1970 SCR (2) 80

[18] STATE OF TAMILNADU V. D.L. PRAKASH Madras high Court (Writ Petition No. 7313 of 2002.)

[19] Regina v. Hicklin, L.R. 2 Q.B. 360

[20] Ranjit D. Udeshi vs State Of Maharashtra 1965 AIR 881, 1965 SCR (1) 65

[21] Section 68 of Information Technology Act - (2) Any person who intentionally or knowingly (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

three years or fine of Rs. Two lakhs. The purpose of inserting Section 68[22] is to ensure complete compliance with the provisions of ITA 2000, rules and regulations made thereunder.

Section 69[23] refers to the offence which has been defined to preserve interests of the sovereignty or integrity of India, the security of the State, friendly relations of the country with foreign state. Controller has been given the power to direct any agency to intercept any information transmitted through any computer resource including computer, computer system, computer network, data, computer database or software.

Section 70[24] provides that any computer, computer system or computer network may be declared to be a protected system by the appropriate Government. The purpose of declaring some systems as protected system could be that such systems are indeed very valuable for the interests of the nation, national security and sovereignty or for public order. Section 70(2) states only limited persons are authorized to access the protected systems. The securing of access or

---

22 *ibid*

23 Section 69 of Information Technology Act - Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

24 Section 70 of Information Technology Act - The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

attempting to secure access to a protected system has been declared an offence punishable with imprisonment of ten years and fine.

Section 71[25], if a Certifying Authority makes a misrepresentation to the Controller or suppresses any material from the Controller for the purpose of obtaining license for becoming a Certifying Authority, this has been declared as a penal offence punishable with imprisonment up to two years or with fine of Rs. One lakh or both. If any person makes a misrepresentation to a Certifying authority for obtaining any Digital Signature Certificate, he shall be punished with two years' imprisonment and one lakh Rs fine.

Section 72[26], if any person has secured access to any electronic record, book, register, correspondence, information, document or other material, then he is duty bound not to disclose the same to any other person. If he does so, shall be punished with two years' imprisonment and one lakh Rs. Fine or both. English courts have also dealt with an issue as to what activities would constitute crime under existing legislation, in the case of **R.V.Fellows and Arnold[27],** it was held that the legislation before the 1994 amendment would also enable computer data to

---

25 Section 71 of Information Technology Act - Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

26 Section 72 of IT Act- Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

27 R.V.Fellows and Arnold, 1997.

be considered a 'copy of an indecent photograph' and making images available for downloading from the website would constitute material being 'distributed or shown'.

Section 73[28] makes publishing of a Digital Signatures Certificate, which is false a penal offence and punishable for two years imprisonment or one lakh Rs fine or both. Section 74 talks of creation, publication, and available of a Digital Signature Certificate for any fraudulent or unlawful purpose. If a person do so he shall be punished with imprisonment of 2 years and fine of Rupee one lakh. Since confiscation is a part of the process of investigation of an offence, Section 76[29], would apply in order to enable the Deputy Superintendent of Police to confiscate. Section 77[30] provides that if any party has been imposed or any confiscation has been under ITA 2000, that does not mean that it would prevent the imposition of any further punishment under any other law, and the person is likely to be punished in accordance with other laws along with violation of provisions of ITA 2000.

Section 79[31], the network service provides would not be liable in all cases of cyber cases. Section 85[32] details the procedure to be followed where corporate entitles or companies commit

---

28 Section 73(2) of IT Act- Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

29 Section 76 of IT Act - Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation.

30 Section 77 of IT Act - No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

31 Section 79 of Information Technology Act - The intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

32 Section 85 of IT Act - Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the

offences or violations. Where a company commits a contravention of any provision of ITA, the company as well as every person in charge of the company shall be guilty of the contravention.

MEASURES TO CURB THE CRIME

Encryption is considered as an important tool for protecting data in transit. Plain text could be converted to ciper text (coded language) by this method and the recipient can decrypt it. The information stored can also be saved in such method. Synchronized passwords schemes used to change the password at user's and host token. The password on such cards changes every 30-60 seconds, which only makes it valid for one tome log-on session. Other methods are signature, voice, fingerprint, identification or retinal and biometric recognition etc. The Firewall method creates a wall between the system and possible intruders. It only permits access to the system to ones already registered with the computer. Using means of cryptography by applying algorithms creates digital Signatures.

CRITICISM

Most of the countries lack enforcement agencies to combat crime relating to Internet and bring some levels of confidence in users. Present law lacks provisions to deter the terrorist groups

company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly

for combatting cybercrimes, as punishments are ineffective, insufficient and only provides three years maximum. However, more effective laws are required at this alarming situation.

CONCLUSION

Society as on today is happening more and more dependent upon technology and crime based on electronic offences are bound to increase. With passage of time and betterment of technology in the present date, has also resulted in number of IT related crimes. Therefore changes are suggested to combat the problem equally fast. Cases liked DAWOOD and QUATTROCHI clearly reveals the problem of enforceability machinery in India. Cryptography is new phenomenon to secure sensitive information. There are very few companies in the present date, which have this technology. Other millions of them are still posed to the risk of cybercrimes.