ISSN: 0976-3570

Cyber Crime and Judicial Response in India

Dr. Abhijeet Deb[1]

I. Introduction :

Advancement of technology not only widens scientific horizon but also poses challenges for the legal system. Computers, Internet and Cyber space are together known as Information Technology. The present challenges for law is to tackle information technology. These challenges are not confined to any single traditional legal category but in almost all categories of law. The existing legal system and frame work have shown inadequacy of while dealing with information technology. It requires new definitions and understanding of the accepted norms of criminal conduct and punishment. The criminal activities in relation to the cyber space can be controlled by framing legal rules, strengthening the administrative frame work and convicting the accused following the quick and efficient justice delivery system. The judiciary throughout the world have been dealing with these problems.

II. Cyber Crime and Legal Provisions:

As internet grows, numerous legal issues arise. One of the most important issues concerning cyberspace today is that of cyber crime. Cyber crimes refer to all the activities done with criminal intent in cyberspace. Cyber crimes mainly include transmission of the pornographic and obscene matters, online harassment, hacking and cyber terrorism. Computer crime can also involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief. The Information Technology Act, 2000 has discussed the issues of cyber crimes in two broad groups. One is Chapter IX which deals with penalties and adjudications under sections 43 to 47 and another is Chapter XI which deals with offences under sections 65 to 75. The Information Technology Act, 2000 deals with the following cyber crimes along with others[2]:

a. Tempering with computer source documents,

b. Hacking,

c. Publishing of information which is obscene in electronic form,

Cyber crimes other than those mentioned under the Information Technology Act :

i. Cyber Stalking,

---

1 Assistant Professor, Jalpaiguri Law College.

2 R. M. Kamble & C. Vishwapriya : "Cyber Crimes and Information Technology", NLR, 2008 – 2009, Vol. 4, No. 1, p. 9.

ii. Cyber Squatting,
iii. Data Diddling,
iv. Cyber Defamation,
v. Torjan Attack,
vi. Financial Crimes,
vii. Internet Time Theft,
viii. Virus / Worm Attack,
ix. E-mail spoofing,
x. E-mail Bombing,
xi. Salami Attack,
xii. Web Jacking.
xiii. Cyber Terrorism.

a. Tempering with computer source documents: Chapter XI of the Information Technology Act, 2000 in a magnificent way tries to cover all most all aspects of cyber crime. Section 65 of the Act provides that 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 be extended up to two lakh rupees, or with both. For the purposes of this section computer source code means the listing of programmes, computer commands, design and layout and programme analysis of computer source in any form.

b. Hacking : Hacking has become associated with the act of obtaining unauthorized access to programmes or data held on computer system. Section 66 of the Information Technology Act, 2000 says that whoever with intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack. Generally there are three types of hackers – i). the amateur group who are the latest technical proficient and confined their activities to prove their capability of penetrating system; ii). the browser group has moderate technical ability and gained unauthorized access to other person's files and iii). the cracker group who has the most technical ability and their activity ranges from copying files to damaging programmes and system.[3]

3 Dr. Sarla Gupta (Agarwal) & Beniprasad Agarwal, Cyber Laws, Premier Publishing Co., Allahabad, 2008

c. Publishing of information which is obscene in electronic form: Section 67 of the Information Technology Act, 2000 provides that whoever publishes or transmits or causes to be published in electronic form, any material which is lascivious or appeals to the prurient interest or its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second and subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

i). Cyber Stalking : Cyber Stalking involves following a person's movements across the internet by posting messages in the nature of threatening on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

ii). Cyber Squatting : Cyber squatting is the practice, by which a person, or legal entity books up the trade mark, business name, or service mark of another entity as his own domain name. It is for the purpose of holding on to it and thereafter selling the same domain name to the other person for valuable premium and consideration. Cyber squatters book domain names of important brands in the hope of earning quick millions.

iii). Data Diddling : This kind of an attack involves altering the raw data just before computer process it and then changing it back after the processing is completed.

iv). Cyber Defamation : Cyber defamation can be defined as any act, deed, word, gesture etc. in cyberspace, designed to harm a person's reputation on the internet or even off-line. Just as everyone in the real world has a right to an inviolate reputation, so is the case in cyber space. This type of crime is similar to cyber-venting, where instead of creating a site, email is being used to defame people.

v). Torjan Attack : Torjan is an unauthorized programme which functions from inside what seems to be an authorized programme, thereby concealing what it is actually doing.

vi). Financial Crimes : A variety of services are offered by the businesses to the consumers through internet. Internet has been misused by the dishonest traders for pertaining fraud and a new species of white-collar crime has come into existence. Internet frauds represent frauds committed by people using any of the services available on the internet. The fraud schemes include all the traditional frauds and some ingenious new ones. These include online auction

frauds, online retail sales frauds, online investment frauds, business frauds, payment card frauds and others.

vii). Internet Time Theft : This connotes the usage by an unauthorized person of the internet hours paid for by another person.

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

ix). E-mail spoofing : A spoofed email may be said to be one which misrepresents its origin. It shows it's origin to be different from which actually it originates. Spoofing is the act of electronically disguising one computer as another for gaining access to a restricted system.

x). E-mail Bombing : Email bombing refers to sending a large amount of emails to the victim resulting in the victim's email account or mail server crashing.

xi). Salami Attack : This attack is used for commission of financial crimes. The key here is to make alteration so insignificantly that in a single case it would go completely unnoticed.

xii). Web Jacking : This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He even mutilate or change the information on the site. This may be done for the political objectives or for money.

xiii). Cyber Terrorism : Cyber terrorism can be defined to be the premeditated use of disruptive activities or threat in cyberspace with intention to further social ideological, religious, political or similar objectives. A cyber crime is a domestic issue but cyber terrorism is a global concern.[4]

III. Judicial Response in India :

The Information Technology Act, 2000 is illustrative of the prevailing confusion in the area of jurisdiction in the context of the internet. Section 1 of the Information Technology Act, 2000 provides for the applicability of this new law. Keeping in mind the universal nature of the impact of computers and internet, the legislature has decided that the Information Technology Act, 2000 shall be applicable to the whole of India including Jammu and Kashmir. Since, the internet

4 Dr. Farooq Ahmad, Cyber Law in India (Law on Internet), 3rd Edn., New Era Law Publications, Delhi, (2008)

is everywhere, the commission of crime by an individual, for example, posting obscene materials to internet, results in the criminal act being simultaneously committed everywhere on the internet. Further, defamatory materials posted by newsgroups on the internet are accessible by persons the world over who access to the internet. In India Chapter XIII of the Code of Criminal Procedure, 1973 deals with the jurisdiction of Courts in respect of criminal matters. It has been structured in such a manner as to enlarge as far as possible, the range of locations in which the offence may be tried in order to minimize impediments to prosecution on the basis of technical objections. The Information Technology Act, 2000 specifically provides that unless otherwise provided in the Act, the Act also applies to any offence or contravention there under committed outside of India by any person irrespective of his nationality.[5] It also clarified that the Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India[6]. But, where the website uses a server or any other computer net work located in India, the Information Technology Act assume jurisdiction to question the website under section 67 of the I.T. Act. Again, where a person from USA or UK hacks a computer system or network in India, section 66 of the IT Act would be applicable to punish the accused for hacking because his act involves a computer in India. Further, where a person anywhere in the world plants a virus into a computer system located in India, he would be liable under section 43(c) of the IT Act, 2000.

The Case of The *State of Tamil Nadu Vs Suhas Katti*[7] is notable for the fact that the conviction was achieved successfully within a relatively quick time of seven months from the filing of the FIR. Considering that similar cases have been pending in other States for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial deserves a special mention.

Mr S. Balu, the Assistant Commissioner of Police in charge of the Chennai's Cyber Crime Cell at the Commissioner's office acknowledged that the assistance provided by Naavi and the Cyber Evidence Archival Center was helpful in the speedy resolution of the case. The case was also notable since it silenced several critics about the inability of the Police in general to be capable of Cyber Crime investigation and more so production of satisfactory evidence to prove the case in a court of law. This case will therefore be considered as a land mark case in the history of Cyber Crime Management in India. The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by

5 Sec. 1(2) of IT Act, 2000
6 Sec. 75 of IT Act, 2000
7 Judgment delivered on 11-5-2204 by CJM, Egmore

the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet. On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C. NO. 4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked.

The Defence argued that the offending mails would have been given either by ex-husband of the complainant or the complainant her self to implicate the accused as accused alleged to have turned down the request of the complainant to marry her. Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court based on the expert witness of Naavi and other evidence produced including the witness of the Cyber Cafe owners came to the conclusion that the crime was conclusively proved.

The court has also held that because of the meticulous investigation carried on by the IO, the origination of the obscene message was traced out and the real culprit has been brought before the court of law. In this case Sri S. Kothandaraman, Special Public Prosecutor appointed by the Government conducted the case.

Honourable Sri.Arulraj, Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows:

> "The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/- and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently."

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of Information Technology Act 2000 in India.[8]

8 http://www.naavi.org/cl_editorial_04/suhas_katti_case.htm

In another case Avnish Bajaj, CEO of Baazee.com, an online auction website, was arrested for distributing cyber pornography[9]. Baazee.com, a customer-to-customer website, which facilitates the online sale of property. Baazee.com receives commission from such sales and also generates revenue from advertisements carried on its web pages. An obscene MMS clipping was listed for sale on Baazee.com on 27th November, 2004 in the name of "DPS Girl having fun". Some copies of the clipping were sold through Baazee.com and the seller received the money from the sale. Avnish Bajaj was arrested under section 67 of the Information Technology Act, 2000 and his bail application was rejected by the trial court. He then moved the Delhi High Court for bail. The issues raised by the prosecution were – i). the accused did not stop payment through banking channels after learning of the illegal nature of the transaction and ii). the item description "DPS Girl having fun" should have raised an alarm. Issues raised by the defense were – i). section 67 of the Information Technology Act, 2000 relates to publication of obscene material and it dose not relate to transmission of such material and ii). on coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend. But, the Court has observed – i). it was not been established from the evidence that any publication took place by the accused directly or indirectly; ii). the actual obscene recording / clip could not be viewed on the portal of Bazee.com; iii). the sale consideration was not routed through the accused; iv). prima facie Baazee.com had endeavored to plug the loophole; v). the accused had actively participated in the investigations; vi). the nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof; vii). even though the accused is a foreign citizen, he is of Indian origin with family roots in India; viii). the evidence that has been collected indicates only that the obscene material may have been unintentionally offered for sale on the website and ix). the evidence that has been collected indicates that the heinous nature of the alleged crime may be attributable to some other person. Basing on the above findings the Court granted bail to Mr. Avnish Bajaj subject to furnishing two sureties of rupees one lakh each and ordered him to surrender his passport and not to leave India without the permission of the Court.

In the case of *Syed Asifuddin and Ors. vs. The state of Andhra Pradesh & Anr.*[10] Tata Indicom employee were arrested for manipulation of the electronic 32-bit number ESN programmed into cell phones that were exclusively franchised to Reliance Infocom.. While delivering the judgement the Court has observed :- i). As per the section 2 of the Information Technology Act, 2000, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and devices which are

9 *Avnish Bajaj vs. State of Delhi*, (2005) 3 Comp, LJ 364 (Del); 116 (2005) DLT 247

10 2005 Cri LJ 4314

programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer; ii). Every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the out going audio signals and incoming signals. This is a microprocessor similar to the one generally used in compact disk of a desktop computer. Therefore the Court held that cell phone is a computer as envisaged under the Information Technology Act, 2000 and when ESN is altered the offence under section 65 of the Information Technology Act is attracted.

In *Frios vs. State of Kerela*[11] it was declared that the FRIENDS application software as protected system. The author of the application challenged the notification and the constitutional validity of software under Section 70 of the Information Technology Act, 2000. The court upheld the validity of both. It included tampering with source code. Computer source code the electronic form, it can be printed on paper. The court held that Tampering with source code are punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.

In *State vs. Mohd. Afzal and others*[12] popularly known as the Parliament Attack case, several terrorists had attacked the Parliament House on 13th December, 2001 intending to take as hostage or kill the Prime Minister, Central Ministers, Vice-President of India and Members of Parliament. Several terrorists were killed by the police in the encounter and several persons were arrested in connection with the attack. The Designated Judge of the Special Court constituted under Section 23 of the Prevention of Terrorist Activities Act, 2002 (POTA) had convicted several accused persons. They filed an appeal in the Delhi High Court challenging the legality and validity of the trial and the sustainability of the judgment. Digital evidence played an important role in this case. Computerized cell phone call logs were heavily relied upon in this case. A laptop, several smart media storage disks and devices were recovered from a truck intercepted at Srinagar pursuant to information given by two of the suspects. These articles were deposited in the police "malkhana" on 16th December, 2001. Although the laptop was deposited in the "malkhana" on 16th December, some files were written onto the laptop on 21st December.

The laptops were forensically examined by a private computer engineer and the Assistant Government Examiner of Questioned Documents, Bureau of Police Research, Hyderabad. The laptop contained files relating to identity cards and stickers that were used by the terrorists to enter the Parliament premises. Cyber forensic examination showed that the laptop was used for creating, editing

11 AIR 2006 Ker.279 ; 2006 (3) KLT 210

12 107 (2003) DLT 385

and viewing image files (mostly identity cards). Evidence found on the laptop included: 1. fake identity cards, 2. video files containing clippings of political leaders with Parliament in background shot from TV news channels, 3. scanned images of front and rear of a genuine identity card, 4. image file of design of Ministry of Home Affairs car sticker, 5. the game 'wolf pack' with the user name 'Ashiq'. Ashiq was the name in one of the fake identity cards used by the terrorists. Issues raised by the Prosecution were : 1. Analysis of the Windows registry files of the suspect laptop showed that its hard disk had not been changed. 2. If internet has been accessed through a computer then the actual date of such access would be reflected. Additionally, if any change is made to the date setting of the computer, it would be reflected in the history i.e. in the REG file. 3. A hard disc cannot be changed without it being reflected in the history maintained in the REG file. 4. It was not possible to alter the date of any particular file unless the system date had been altered. 5. The files written on the laptop on 21st December were "self generating and self written" system files. These were created automatically by the laptop's operating system when the laptop was accessed by law enforcement agencies at the "malkhana". Issues raised by the Defence were : 1. Although the laptop was deposited in the Government "malkhana" on 16th December, some files were written on the laptop on 21st December. 3. The date setting on a computer can be edited. 4. In the absence of verified time setting and reliable information about the hard disc being original, there is no certainty that the material found on a later date, was exactly the material, which may have existed on a previous date. 5. Hard disc is a replaceable component and could be formatted. If a hard disc was replaced, it would not contain the data which was stored earlier unless it was re-fed. 6. The Windows registry files can be edited. 7. The back up of complete suspect hard disc was not taken by the law enforcement agencies. 8. The date setting on a file is related to the date setting on the computer. It is possible to modify this date. 9. Information stored in a computer is on a magnetic medium which can easily be polarized. Therefore, any data in a computer can be changed by a knowledgeable person. 10. The date of last access to a file is treated differently by different software. The time of last access was meaningless in the absence of knowledge as to what software is used to process the file. 11. Software which was installed in a computer could be modified and un-installed without leaving any trace.

Though the accused had argued that computers and digital evidence can easily be tampered and hence should not be relied upon the Court dismissed these arguments. It said that challenges to the accuracy of computer evidence on the ground of misuse of system or operating failure or interpolation, should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

Cyber crimes must be declared as "federal crimes" and "included in List 1 (Union List) of the Seventh Schedule of the Constitution," the Chief Justice of

the Karnataka High Court, N.K. Sodhi, has said. If this is done, cyber crime will then be brought under the purview of Article 246 (1) of the Constitution. Articles 245 to 254 of the Constitution deal with the distribution of legislative powers between the Union and the States. Article 246 says Parliament has "exclusive powers to make laws" with respect to any matter detailed in List 1 of the Seventh Schedule of the Constitution. Cyber terrorists, Mr. Sodhi said, need no weapons and can remain anonymous. They can hack into a hospital network to alter patients' prescriptions and kill them or gain access to an airport's computer system and, by simply changing a decimal point, vary the altitude of aircraft causing them to collide. Information technology can speed up work in the judiciary, he said. The United States, Singapore, Australia, and the United Kingdom use IT extensively. In Andhra Pradesh, he said, undertrials are produced before magistrates using video links and this brings in transparency and accountability.[13]

IV. Concluding Remark:

To control this crime legislature has passed a law that is Information Technology Act 2000. It is worth mentioning that Indian information Technology Act 2000 does not deal with the cyber Defamation and therefore we have to rely on Indian penal code. Internet defamation can take place on net, through any one of the following communication avenues: email, web site postings, chat rooms, etc. As we all are aware that defamation is an offence according to IPC. Section 499, which consists of following essentials: 1. Making or publishing an imputation concerning any person, 2. The imputation is made with the intention of causing harm to, or knowing or having reason to believe that such imputation will harm the reputation or such person. But, there are certain other issue which is needed to be improved. That is jurisdiction. A court must have the jurisdiction, venue and appropriate service of process in order to hear a case and render an effective Judgment. The Constitution has, by Article 247, clothed Parliament with Power to provide for the establishment of additional courts for the better administration of laws made by parliament.[14]

Problem do arise when transactions through the internet between parties coming from various parts of world and has virtual nexus. Under such circumstances if one party wants to sue another, then the question arises as to where he can sue? Traditional principles cover two areas- firstly, the place where the defendant resides, or secondly, where the cause of action arises. In context of internet all these things are difficult to establish. Sections 13 (3),(4),(5) of Information Technology Act, 2000 really created some sort of confusion. The

13 The Hindu, Online edition of India's National Newspaper, Monday, Jan 31, 2005 http:\\cyber crimes\The Hindu Karnataka News Declare cyber crime a federal offence Sodhi.htm

14 M.P. Jain, Constitution of India, 5th Edn., Wadhwa and Company, Nagpur, (2005)

provisions say: Sec 13 (3) : save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business and is deemed to be received at the place where the addressee has his place of business; Sec 13 (4): the provision of sub section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have received under sub-section (3) and Sec 13 (5) for the purpose of the section: if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business. If the originator or the addressee does not have a place of business his usual place of residence shall be deemed to be the palace of business.

It could be said that the aforesaid sub-section (3), (4) and (5) of section 13, being deeming provisions, shall apply only for the purposes of the Information Technology Act, where as for the application of the concept of cause of action; under our civil law, only the places from where the parties actually interact by dispatch and receipt of electronic records shall be considered in all cases. This is still an unsettle thing and we have to wait till the High Courts and the Supreme Court take any final decision.

Further, section 75 of the Information Technology Act provides that this Act shall apply also to offence or contravention committed outside India by any person irrespective of his nationality. The wording of the section is such that the almost brings the whole world within the Jurisdiction of the Indian court. In such case one question arises that the Indian court has such a wider jurisdiction. Moreover, the most cyber crimes are bailable offence, corporations can forget about being able to get their errant employees, who misuse confidential data and information behind bars. The maximum damage by way of compensation stipulated by new cyber law amendments is Rs.5 crores. When calculated in dollar it turns to a small figure and hardly provides any effective relief to corporations, whose confidential information, which might be worth several crores, is stolen or misused by its employee.

The other demerit is that the word Spam is not mentioned in the Information Technology Amendment Bill. This is a serious problem because India already features among the top 10 nations in the world from where Spam originates. Therefore, Indian Courts urgently require the relevant provisions in I T Act to check the menace of spam related cyber crimes.

The amendment to the Information Technology Act does not address jurisdictional issues. At a time when internet has made geography history, it was hoped that the new amendments would throw light on complicated issues pertaining to jurisdiction. This is because numerous activities on internet take place in different jurisdiction. So, there is need of law to control the Jurisdiction.

The new amendments are likely to impact all industries which use

computers, computer systems and networks and data and information in electronic form. These reasonable security practices and their mandatory adoption would aid better regulation but are also likely to unveil a package of unpleasant surprises for many. The IT Amendment Bill 2008, which has been passed by lok Sabha is appeared to have been passed in haste. So, the legislature must take it in to consideration.

Further, cyber laws enacted in one country may counteract with another's notions of national sovereignty, jurisdiction, human rights and privacy. Therefore, it may be argued there should be an international body which should ensure that all the cyber criminals are taken to task. This impartial body should be vested with the universal jurisdiction. It is one of the ways through which the harmonization can be possible as a single body would be entrusted with the task of dealing with the cyber crimes effectively and globally.