EMERGENCE OF CYBER CRIMES: A CHALLENGE FOR THE NEW MILLENNIUM

Mr. Kush Kalra*

Abstract

With new mediums of communication, business and societal activities, growth of Newer and varied kinds of crime are inevitable. Computers with the aid of the Internet Have today become the most dominant medium of communication, information, Commerce and entertainment. The Internet is at once several shopping malls, Libraries, universities, newspaper, television, movie theatre, post office, courier Service and an extension of government and business. It is like life in the real world being extended and carried on in another medium that cuts across boundaries, space, time, nationality, citizenship, jurisdiction, sex, sexual orientation, and age. The Internet, with all the benefits of anonymity, reliability, and convenience has become an appropriate breeding place for persons interested in making use of the Net for illegal gainful purposes, either monetary or otherwise Since anything related to the Internet was being prefixed with the word 'cyber'[1] the However, the word 'cyber-crime', by its very terminology, restricts itself to the offences committed on the Internet. The term is liable to be given a restricted meaning. It is for this reason that the authors have preferred the word 'computer-crimes' rather than 'cybercrimes' which, in its wider ambit, would encompass offences committed in relation to or with the help of computers. Defined broadly, the term 'computer crime' could reasonably include a wide variety of criminal offences and unlawful activities related to or having connection to computers. The potential scope is even larger when using the frequent companion or substitute term 'computer-related crime'.

Introduction

In the present times, the forms of crimes have multiplied manifold because of advent of new technology and expansion of human

* Assistant Professor, Delhi Metropolitan Education (Affiliated to GGSIP University), Noida.

1 Cyber: A prefix used in a growing number of terms to describe new things that are being make possible by the spread of computers.

activities in diverse areas. Criminals are transgressing national boundaries with ease. On the one hand scientific and technological advancements have provided opportunities for growth and development of individual and community interest; at the same time these also provide a breeding ground for malefic finds to undertake unethical and unlawful activities. Such unscrupulous and anti-social behaviours are always a step ahead of the combating measures and mechanism adopted by the law enforcement authorities. The information technology has given a boost to data processing in organized and productive manner. It has also opened a new era of communication across the world. The computer is being used to create, transmit, retrieve and store information in the electronic form replacing the paper documents. Internet has entered the house of a common man its users are adding up every day at a fast rate. We are also witnessing dependence on computer and internet in the commercial and the utility services. Consequently, emerging cyber-crimes are not only posing threat to the commercial world but also to the interest of the internet community and a common man at large.

Now the word 'Cyber' is not new to us. It is used to denote a virtual space or memory. It seems to have come from 'Cyber Space'. This was first used in 1984 in William Gibson's novel *Mecromancer* which was a scientific fiction. The author used this phrase to denote the online world of computers. When we put this word cyber with crime that is cyber-crime it means the criminal act/crime committed in the online world of computer.

There is no exhaustive definition of cyber-crimes. It could cover activities which basically offend the human sensibilities, for example, hacking and child pornography. Cyber-crimes may include any criminal act dealing with computers and Internet. This may also include traditional crimes committed through Internet, like Internet frauds, when the computers and internet are used as tools to commit an act which is otherwise an offence. A broad definition would be any crime committed that involves the use of a computer. In the current times, this would mean just about every crime committed, should a criminal use a computer to keep track of robberies he has committed or the drugs he has sold.[2] Therefore, in the commission of computer crimes the computer or computer network is used as a tool or a target.

---

[2] Paul A. Curtis, Sergeant-Arkansas State Police, Criminal Justice Institute, Director Dr. Lee Colwell School of Law Enforcement Supervision, "Cyber Crime: The Next Challenges Faced by Law Enforcement, While Investigation Computer Crimes in the Year 2000 and Beyond".

Since the first reported case of computer abuse in 1958, computers have been involved in most types of crimes including theft, burglary, larceny, fraud, embezzlement, extortion, sabotage, espionage, kidnapping and murder. We must include the crime of child pornography as well.[3] Also computer systems themselves can be the target of attack when a computer virus is unscrupulously introduced into the systems to alter, damage or destroy data. The cyberspace is hinting a new environment of various activities ranging from business, commerce, administration, entertainment etc. hence the related legal issues are cropping up. Since crime is a deviation from the normal behaviors, such deviations are bound to emerge in cyber space. In view of the expanding canvas of anti-social and unethical activities involving use of computers and computer networks, paramount task is to make a comprehensive study to precisely define specific cyber-crimes and to provide penal sanctions for them.

At the present juncture precise definitions of specific cyber-crimes need to be worked out. These must specifically provide for required *actus reus* and *mens rea*. Another important aspect is to provide an effective enforcement frame work. That is need for efficient enforcement agencies to deal with new type of criminality. Surmounting of jurisdictional issues is another major challenge in dealing with these crimes. However, because of peculiar features of cyber-crimes it is not easy to tackle these issues. Some of the hurdles and difficulties may be identified as under:

a. Anonymity of computer network

A network user/surfer can easily conceal his/her identity. This not only makes the task of detecting computer crimes and computer criminals more difficult but it also complicates the task of collection of evidence and its subsequent proof at the trail. Loss of evidence is very common problem as the extracted data are routinely destroyed.

b. Changed nature of crime

The crimes committed in the physical world are different from the crimes committed in the virtual space. The laws applicable on the traditional crime are not applicable to cyber-crimes. For example, difficulties will arise in the prosecution of individuals for the theft of information because common law/Indian Penal Code requires proof of taking away of stolen property. It is not possible to

[3] *Ibid.*

provide the proof of taking away of information if theft is committed through internet. Similarly, concepts of trespass and breaking in do not fit into the cyber world because there is no physical entry into the computer and therefore no criminal trespass can be committed in cyber space as per definition under Indian Penal Code.

c. Cyber-crimes are borderless

Cyber-crimes are not limited in national boundaries. These crimes may be committed in many jurisdictions at the same time. Defamatory, malicious, pornographic material if posted on a web-site is accessible globally. It becomes difficult or sometimes impossible to investigate and prosecute such offences due to inaccessible jurisdiction. It is said that a computer criminal is here, there, anywhere, everywhere yet nowhere. Thus jurisdiction is highly debatable issue as to the maintainability of any civil action or cyber crime as due to expanding cyber space the territorial boundaries are vanishing. The concept of territorial jurisdiction as envisaged under Section 16 of the Civil Procedure Code and Section 2 of the Indian Penal Code are becoming irrelevant.

d. Easier to store, retrieve, transfer and delete information

Electronic information used in cyber-crimes is cheaper to produce, easier to store, transmit and eventually delete quickly. For example a file containing defamatory or porn material can be easily and quickly sent to any number of persons just sitting in a chamber with a click of mouse. The access is easier too in a similar manner. In these circumstances task of law enforcement becomes very difficult.

Types of cyber jurisdiction

Problems regarding cyber jurisdiction is faced in the following areas or matters:

1. Cyber jurisdiction in civil matters
2. Cyber jurisdiction in criminal matters
3. Cyber jurisdiction in international cases
4. Internet warnings issued by different authorities

1. Cyber jurisdiction in civil matters

Cyber jurisdiction in civil matters mainly comes into picture when a Website or any information hosted on the Internet leads to commitment of a civil wrong in another State. In deciding whether jurisdiction exists over a defendant, the U.S. Federal Courts apply

the law of forum States subject to the limits of the due process clause of the fourteenth amendment. This is illustrated in the following cases:

In *Bensusan Restaurant Corp. v. King*,[4] the Court at New York "agreed finding that it took several affirmative steps to obtain access to the Website and use the information there.....The Court also ruled that there was no prove (sic) that the defendant had directed any infringing activity at New York Id. They held that merely because someone can access information on the Internet about an allegedly infringing product, it is not equivalent to a person selling, advertising, promoting or otherwise attempting to target that product in New York Id."[5] Therefore, the Court in New York lacked jurisdiction in this case. Here the plaintiff, the operator of New York club claimed that the defendant, owner of an operator of small club in Columbia, had violated his rights by using its trademark. Whereas the defendant claimed that Website was created at Missouri and was aimed at residents at Missouri, and if the ticket is sold on Internet, the buyer has to pick the ticket at outlet in Columbia or at the club at the night of the show. Creating a Website was similar to putting a product in the filed of commerce and its effect could be national or international but it does not amount to an act that was purposely directed toward the other State. Therefore, it is not sufficient for the other State to exercise its jurisdiction.[6]

In *McDonough v. Fallon McElligott*[7], defendant from outside California created a Website which was accessed by a Californian. Subsequently, dispute arose and the matter had gone to the Federal Court. In this case, the "federal Court in California also refused to exercise personal jurisdiction over the defendant simply because it maintained a Website. The Court Held that the fact that the defendant had a Website accessed by Californians was not enough by itself to establish jurisdiction."[8]

In *Zippo Mfg. v. Zippo Dot Com*, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997), the Court differentiated between active and passive Website and held that a passive Website that only makes information available to the Internet user is not sufficient ground for exercising the jurisdiction. Whereas, an active Website, i.e., a

---

4 937 F Supp. 295, (S.D.N.Y. 1996).
5 http://www.asianlaws.org/projects/cc_jurisdiction.htm#3.
6 Suri, R.K. & Chhabra, K.N. Cyber Crime, Pentagon Press, New Delhi, 2002, p.73.
7 Inc., 1966, Dist. LEXIS 15139, No: 93-4037, Slip op [S.D. Cal. Aug 6, 1996].
8 http://www.asianlaws.org/projects/cc_jurisdiction.htm#3.

Website that entered into contracts and knowingly and repeatedly transmitted computer files would be properly subject to personal jurisdiction. In cases dealing with the middle ground, where interacted Websites exchange information with a user, the exercise of jurisdiction should be determined by examining the commercial nature of the exchange and the level of interactivity.[9]

Here the defendant's Website, which rendered Internet news service, registered the domain names, i.e. "Zippo.com", "Zippo.net" and "Zippo-news.com." It was having more than one lakh subscribers all over the world out of which roughly 3000 were in Pennsylvania. Further the defendant had entered into agreement with seven Internet access providers in Pennsylvania. The plaintiff sued the defendant for trademark dilution, infringement and false designation for using the domain names.[10] Here the Court held that it has personal jurisdiction that depends upon entity's presence on Internet. The Court found that entity's presence on Internet is directly proportionate to the nature and quality of commercial activity on the Internet.[11]

2.Cyber jurisdiction in criminal matters

Initially cyber jurisdiction was an issue in civil cases only. But in 1966 in *U.S. v. Thomas* cyber jurisdiction became an issue in criminal cases also. In this case, defendants (a couple) operated a pornographic bulletin board from their home in California in 1991 which was accessed by members having password, which could be selected, retrieved and downloaded on their own computers. In appeal the U.S. District Court, Tennessee, upheld the conviction under the statute which prevents the channels of inter State commerce from being used to disseminate obscene matter. The Court applied the Contemporary Community Standard as was done in *Miller v. California*,[12] explaining that obscenity was to be judged by what the average person applying contemporary community standards would find to be obscene.[13] And in this case matter was not obscene under California Bay Area standards but was so under the standards of Tennessee. The Court applied the standards of geographical area where the material was sent.[14]

---

9 http://www.asianlaws.org/projects/cc_jurisdiction.htm#3.
10 Rao, S.V. Joga, *Law of Cyber Crime*, Wadhwa& Company, Nagpur, 2004, pp. 43-44.
11 Suri, R.K. & Chhabra, K.N. *Cyber Crime*, Pentagon Press, New Delhi, 2002, p.76.
12 413 U.S. 15, 93 S.Ct. 2607, 37 L.E.D. 2d.419 [1973].
13 http://www.asianlaws.org/projects/cc_jurisdiction.htm#3.
14 Suri, R.K. & Chhabra, K.N. Cyber Crime, op. cit., p. 79.

Defendants argued the Internet environment provides broad ranging connections among people in cyberspace, as such the notion of obscenity tied to geographic locale would put a chill on protected speech. The Defendant's asserted a more flexible definition was needed because BBS operators could not select who received their material.

In *Minnesota* v*. Granite Gate Resorts*,[15] the Minnesota's Attorney General had asserted the right to regulate the activities of an online gambling service based in Las Vegas, Nevada. The Attorney General argued that the defendant had explicitly misrepresented its services as lawful on its Web Page. They denied the defendant's plea to dismiss for lack of jurisdiction because of hits from Minnesota at the defendant's Website, the availability of a toll free number advertised on its Web Page that users could call and the number of Minnesota's residents who had signed on to the defendant's mailing list. The Court held that the defendant's advertising on the Internet constituted a direct marketing campaign at residents of the State of Minnesota and was sufficiently purposeful to subject the defendant to suit in the forum state.[16]

3.Cyber jurisdiction in international cases

In *Asahi Metal Industry Co.* v*. Supreme Court*[17], the U.S. Supreme Court gave the principal of higher jurisdictional threshold when defendant is a foreign national as compared to when he is a U.S. citizen. Here defendant's headquarter was in Japan, the Court refused to exercise the jurisdiction due to following reasons: a) Distance between defendant's headquarter in Japan and Supreme Court of California and "burden of submitting a dispute between two foreign nationals in a foreign legal system," b) California's and foreign plaintiff's slight interest in having the case heard in California, and c) The effect on the "procedural and substantive interests of other nations by California's assertion of jurisdiction over a foreign national."[18]

In *Care Vent Corp.* v*. Nobel Industries*[19] dispute was between California Corp. (plaintiff) and five Swedish citizens and three Americans citizens (defendants) for publishing articles containing false and misleading comparison between Core Vent Corp. and

---

15 Inc., 65 USLW 2440, 1996 WL 767431 [D. Minn. Dec 10, 1996].
16 http://www.asianlaws.org/projects/cc_jurisdiction.htm#3.
17 480 U.S. 102 (107 S. Ct. 1026) (1987).
18 Suri, R.K. &Chhabras, K.N. *Cyber Crime*, Pentagon Press, New Delhi, 2002, pp. 81-82.
19 AB, 11 F 3d 482 (9th Cir 1993).

Nobel Parma's Dental implants. The US Court of Appeal upheld the dismissal by U.S. District Court, Central District of California due to lack of jurisdiction. The appellate Court held that California's statute allowed the Courts to exercise jurisdiction over the defendants to the extent permitted by due process clause in United States Constitution, which provides that where there is no systematic and continuous contact between foreign defendants and the State then three pronged minimum contacts test should be applied to decide jurisdiction in the case. The tests are: a) whether there was purposeful availment, i.e., whether the non-resident defendant had purposefully directed his activity or entered into interaction with the forum State or resident or had performed some act by which he got some privilege of conducting some activity in the forum State, b) whether the claim arises out of or is related to defendants activities, and c) whether the exercise of jurisdiction leads to fair play and substantial justice.[20]

Further in *Playboy Enterprises, Inc.* v. *Frene*,[21] the defendant operated a subscription electronic bulletin board which downloaded the unauthorized copyrighted photographs of the plaintiff. The Court held that unauthorized uploading of photographs by the defendant knowing that they could lateron be downloaded by the subscribers' amounts to distribution.[22]

In *Playboy Enterprises, Inc.* v. *Chuckleberry Publishing, Inc.*,[23]the important question for consideration was whether the United States Court has jurisdiction for enforcing the injunction passed on June 26, 1981. The defendant had a pay Website located in Italy which was accessed in the U.S. As subscribers who have a password provided by the defendant at the request of the subscribers were United State citizens, and they were allowed to access the Website, so the data could be downloaded by them. The Court held that it had jurisdiction in enforcing the injunction against the defendant restraining it from publishing and distributing its magazine in the United States.[24]

In *CompuServe, Inc.* v. *Patterson*, 89 f. 3d 1257 (6th Circular 1996) the defendant, a software programmer sold his software to12 Ohio

---

[20] *Id*. pp.82-83.
[21] 839 F Supp. 1552 (M.D. Fla. 1993).
[22] Ryder, Rodney D. *Guide to Cyber Laws: Information Technology Act, 2000*, E-Commerce Data Protection and the Internet, Wadhwa and Company, Nagpur, 2001, p.535.
[23] 939 F. Supp. 1032 (S.D.N.Y. 1996).
[24] Ryder, Rodney D. *Guide to Cyber Laws: Information Technology Act, 2000*, E-Commerce Data Protection and the Internet, Wadhwa and Company, Nagpur, 2001, pp.534-535.

residents through CompuServe registration system where it was clearly provided that the agreement was subject to jurisdiction in Ohio. CompuServe filed a suit claiming that it has not violated the defendant's trademark. The question of jurisdiction arose and the Court observed that the defendant had entered into Shareware Registration Agreement with CompuServe where it had agreed to be governed by the Ohio Law. Then he sent his software to CompuServe system in Ohio and he advertised that software by regular mail message also. The Court held that the defendant by doing so had purposely availed himself of the privilege of doing business in Ohio. Hence the Court had jurisdiction.[25]

In *Inset Systems, Inc.* v*. Instruction Set*, Inc., 937 F. 161 (D. Conn. 1996), plaintiff (Connecticut) claimed that his trademark 'Inset' was infringed by the defendant by using domain name 'Inset.com.' Defendant (Massachusetts based corporation) created a Website accessible by anyone on the web. The Court, while answering the question of jurisdiction held that "(defendant) Instruction has directed its advertisement activity via the Internet...toward not only the State of Connecticut but to all States...Advertisement on the Internet can reach as many as 10,000 Internet users within Connecticut alone, (Defendant) has therefore purposefully availed itself of the privileges of doing business within Connecticut,"[26] and therefore, Court can have jurisdiction.

Again in *Maritz, Inc.* v*. Cyber Gold*,[27] Inc., plaintiff, a Missouri Company sued defendant based in California for registering the domain name "Cyber Gold.com" as it amounted to trademark infringement. Here plaintiff claimed that by providing information about the Company and then providing a personal electronic mailbox and forwarding advertisements and other related information to the selected users in Missouri, defendant was having customers from Missouri and doing business. The Court in Missouri held that Missouri's Long Arm Statute permitted jurisdiction over a non-resident when either there is any business transaction or commission of any tortuous act in that State. The Court while considering Internet similar to telephone or mail but more efficient, quicker and vast means of communication held that this activity of giving advertisement on the Internet and then accessing cyber gold Website by the interesting users is not passive. If a Missouri resident would mail a letter from to cyber gold in California regarding some information regarding its

---

[25] Rao, S.V. Joga, *Law of Cyber Crimes*, Wadhwa & Company, Nagpur, 2004, p.40.
[26] *Id*. p. 41.
[27] 947 P Supp. 1328 (E.D. Mo. 1996).

service. Cyber gold would have option as to whether to mail information to the Missouri resident and would take some effective measure to respond to the mail. As cyber gold responded to each and every Internet user who accesses its Website so its contacts are of such a nature and quality permitting exercise of personal jurisdiction over the defendant.[28]

Further, in a defamation case, *Telco Communication* v. *An Apple a Day*,[29] the United States district Court of Virginia, had Jurisdiction over the Missouri defendant. Here the Virginia plaintiff sued the Missouri defendant for defamation in Internet Press release due to which the plaintiff's stock prices suffered. The Court held that the Press releases were advertisements and, therefore, a solicitation of business over the Internet.[30]

Minnesota Attorney General's warning regarding the Internet

In the United States, some States like Minnesota, California and Texas have taken proactive steps toward matters related to jurisdiction on the Internet. For instance, gambling appears to be a popular criminal activity on the Internet. The Minnesota Attorney General observes that there are a number of services outside of Minnesota that offer Minnesota residents the opportunity to place bets on sporting events, purchase lottery tickets, and participate in simulated casino games. However, these services are illegal in Minnesota.[31]

The Minnesota Office of Attorney General has created a Website to control criminal activity on the Internet where it has published a list of lawsuit summaries and memo on jurisdiction. The Minnesota general criminal jurisdiction statute provides that a person may be convicted is the person 1) commits an offence in whole or in part within Minnesota or; 2) is out of Minnesota but causes, aids or abets another to commit a crime within a State; 3) though outside the State but intentionally causes a result within the State prohibited by the criminal law of Minnesota. Further in *State* v. *Red lake DLF Committee* (303 N. W 2d 54) Minnesota Supreme Court held that the State has jurisdiction over his committee which has purchased advertising space in newspaper for political advertisements.Important question under consideration was whether the Committee was to be registered

---

28 Rao, S.V. Joga, *Law of Cyber Crime,*Wadhwa& Company, Nagpur, 2004, pp.42-43.

29 Civ. Act. No. 97-542-A (E.D. Va. 1997).

30 Kamath, Nandan, Law Relating to Computers, Internet and E-Commerce, Universal Law Publishing Company Pvt. Ltd., New Delhi, 2004, p.39.

31 http://world.std.com/~goldberg/minn.html.

under State law. The Court held that if a person, outside Minnesota, disseminates information within Minnesota through the Internet and produces same result in Minnesota then it becomes the subject of Minnesota civil and criminal law.[32]

Whereas, the Office of the Attorney General of Texas also issued an opinion on the legality of Internet gambling. He opined that playing of a card game by two or more persons by using computer and modem at a private place does not violate criminal law but if the same activity is done through public access or a bulletin board service assisting such a game and charges for service are taken, then it amount to violating various provisions of the Penal Code.[33]

However, California enacted Assembly Bill 2230 where it has extended its jurisdiction of existing law of California-which regulates the sale, lease, or offering for sale or lease of goods or services by telephone, mail order, or catalog—to the out of State vendors who use the Internet or any other electronic means of communication to advertise, selling lease goods and services. Vendor outside California are required to provide specific refund and return policies and make certain disclosures to Californian purchasers. A violation of these provisions is an offence and the bill imposes a state-mandated local program.[34]

Indian position regarding cyber jurisdiction

In cyber world every State should have its national law having extraterritorial jurisdiction to cover extraterritorial character of cyberspace activity as there is no international instrument relating to cyber jurisdiction. Covering this aspect among others, the United Nations Commission on International Trade Law (UNCITRAL) adopted a model law on e-commerce in 1996 which was adopted by the General Assembly by its Resolution No.51/162, dated 30.1.1997. The General Assembly recommended that all States should give favourable consideration to the said model law on commerce. India being signatory to said model law enacted The Information Technology Act, 2000 to make law in tune with the said model law.

One of the biggest drawbacks of the IT Act, 2000, is that it didn't talk about jurisdiction of the Courts in the cyber world. It means

---

[32] Ryder, Rodney D. *Guide to Cyber Laws: Information Technology Act, 2000*, E-Commerce Data Protection and the Internet, op. cit., pp.529-530.

[33] *Ibid.*

[34] http://info.sen.ca.gov/pub/95-96/bill/asm/ab_3301-3350/ab_3320_bill_960617_amended_sen.pdf.

the present law of jurisdiction of physical world is applicable to the cyber world as well. In India, Sections 15 till 20 of the Indian Civil Procedure Code (C.P.C), 1908, and Sections 177 till 188 of the Indian Criminal Procedure Code (Cr.P.C.), 1973, deal with civil and criminal jurisdiction respectively. Under the Cr.P.C., territorial jurisdiction depends upon the place where offence or part of the offence is committed.

Under the C.P.C, the territorial jurisdiction is based upon: (i) place of residence of the defendant, and (ii) place where cause of action arises. But in the cyber world there may be more than one place of cause of action, such as place of cause of action may be a place where a Website is accessed, or place where server is located or place from where an electronic record is sent or place where an electronic record is received. However, the IT Act, 2000, time and place of dispatch and receipt of electronic record is defined.[35]

Section 75 of the Information Technology Act, 2000 extends jurisdiction of Indian Courts to an offence or contravention committed outside India by any person irrespective of his nationality.[36] Further, this law is to apply to an offence or contravention committed outside India by any person if the act or

---

[35] **Section 13 (1)**: Unless and until there is an agreement between the originator (a person who is sending electronic record) and the addressee (a person who is receiving an electronic record), the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator. (2) Unless and until there is an agreement between the originator (a person who is sending electronic record) and the addressee (a person who is receiving and electronic record), the time of receipt of electronic record shall be determined as follows: (a) if the addressee has designated a computer resource for the purpose of receiving electronic records, --(i) receipt occurs at the time when the electronic record enters the designated computer resource; or (ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee; (b) if the addressee has not designated a computer resource alongwith specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee. (3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be displaced at the place where the originator has his place of business, and is deemed to have been received at the place where the addressee has his place of business. (4) The provision of sub-section (2) shall apply notwithstanding that the place where computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section(3). (5) For the purpose of this section:- (a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business, (b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business; (c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

[36] The Information Technology Act, 2000: Bare Act, Universal Law Publishing Co. Pvt. Ltd.www.unilawbooks.com, Delhi, 2004, p.29.

conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.[37]

For example, Mr. Z, an Australian national, residing in USA, gains unauthorized access to a computer located in China and deletes information. Mr. Z has used a computer located in India to gain the unauthorized access. Mr. Z will be liable under the provisions of the IT Act, 2000.[38]

The main difference between the Indian Penal Code and the IT Act, 2000 with regard to extraterritorial jurisdiction, is clarified by way of the following example. If a U.K. national Briney Spears, legitimately procures weapons from India and uses the same for committing a criminal act in the United Kingdom or any other country in the world then she would not be liable for any offence in India as per the IPC. However, if Britney Spears were to use a computer located in India to hack the U.K. government's Website or commit any other offence under the IT Act, 2000, then she will be liable for that offence in India.[39]

Worldwide impact of cyber-crimes

1. The global scenario

There is great concern world over regarding various types of crimes being committed through computers and the Internet. Almost every day there is an international story about some or other portal that has been attacked, credit card fraud, or some various bringing down the system. Business is the prime target-but public authorities and even individuals are vulnerable too.

It has been generally acknowledged by experts that there is hardly any computer in the world that is hacking proof. The most mentionable of these cases was the 'denial of service' of giants like Yahoo.Com, Buy.Com, Amazon.Com, eBay, the shutting down of the website of World Trade Organization, 'stealing of *www.web.net* and *www.bali.com*, the infamous losses caused by the 'I Love You' virus and 'Mellisa' virus, among others.

A survey of US business firms showed that 85% of those covered had at some time been targeted by hackers. In Great Britain, a report by the Communications Management Association (CMA)

---

37 http://www.cyberpolicebangalore.nic.in/ch11_75.htm.
38 http://www.asianlaws.org/cyberlaw/library/india/general/jurisdiction_act.htm.
39 *Ibid.*

states that a third of the country's major businesses and public authorities have been hit. In the US, the Pentagon's system alone was attacked more than 22000 times –in one year. And the FBI has identified 5000 systems as being "highly vulnerable" to cyber-crime, which has –according to Ronald L. Dick, the FBI's new director-the capacity "to destabilize a country's whole economy".[40]

Gauging the economic impact of cyber-crime is complicated by the fact that reported offences are merely the tip of the iceberg. Several studies carried out in Europe and the US suggests that only a third of the victims call in the police. Credit card fraud is thought to cost some 400 million dollars every year- and virus attacks some 12 billion. Finally, profits lost by firms whose patents and trademarks are stolen reportedly amount to 250 billion dollars every year, or nearly 5% of world trade...[41]

2. Indian scenario

Computer crimes had not emerged as a major problem area of the law enforcement agencies in India until recent past. The main reason for low incidence of computer-related crimes in India was that computerization of banks and other financial institutions were still in early stages. Further, the networking of computers had not yet taken place in any big way in the sensitive sectors which could be vulnerable to theft and alteration of data. But as the process of computerization has now picked up significant increase in computer crime is expected in the near future.[42]

Cyber-crime has now become a reality in India. Difficult to detect, seldom repeated and even more difficult to prove, computer-related crime lacks traditional paper audit trail, is away from conventional policing and requires specialists with a sound understanding of computer technology. Furthermore with the country posed to enter the information superhighway-over three million computers in place-and industry and banks networked, the realization of the dangers and threats is finally sinking in.[43]

The major areas of concern, which are highly vulnerable to computer crimes, include critical infrastructures like banks and

---

[40] *Available at*: http://www.coe.int/T/E/Communication and Research/Press/Themes/Files/Cybercrime e cybercrime.asp, "Cyber Crime – The Target it Hits, The Damage it Does", Visited on 21 December, 2009.

[41] *Ibid.*

[42] Balwinder Singh (2000): "Cyber Crime – A new Challenge for the Police." In: *CBI Bulletin*, (February).

[43] Krishna Kumar (2001): *Cyber Laws-Intellectual Property* and *E-Commerce Security*, New Delhi: Dominant Publishers, pp. 295-308, at 295.

other financial institutions, telecommunications, airlines, railways, power sector and other crucial departments of both the Government of India and numerous States etc.

Regards incidents of computer crimes in India, a few examples would give an idea about the nature of cases which have occurred so far.

- In New Delhi Municipal Corporation, a private agency entrusted with the responsibility of preparing and collecting electricity bills, embezzled Rs. 6.5 crore by creating duplicate set of bills showing lower receipts.
- In Railway Computerised Reservation System, a few cases of false accounting by wrongly categorizing upper class seasonal tickets have come to notice.
- Subscribers of Videsh Sanchar Nigam Ltd.'s (VSNL) Internet service in Mumbai were pleasantly surprised on the morning of 2 March, 1999 as they received an e-mail from Mr. Amitabh Kumar, the acting Chairman and managing Director of VSNL, stating, VSNL's aggressive price cuts. From Rs. 3500 for 100 hour account the rates were down from Rs.10000 to Rs. 6500. However the e-mail turned out to be nothing but the first instance of a system break-in at VSNL that hurt its pride.
- Indian Airlines was defrauded of several lakh rupees when open-ended tickets for shorter sectors were issued in fictitious names by some staff members. Computer records were tempered with to show longer sectors and refunds obtained.
- In the Purulia Arms Drop Case, the main players used the Inernet extensively for international communications, planning and logistics.
- The websites of Parliament, Zee TV etc. have also been broken into by anti-India hackers at one time or the other.

Above mentioned are some of the instances which indicate the vulnerability even of the most sophisticated computer networks to hacking and cracking. These instances also amply demonstrate the ability and reach of cyber-criminals and hackers to manipulate the system and walk away freely from the long arm of the law. Hence there is a pressing need for stringent cyber laws to deal with the problem of such magnitude and dimension. It is about time that we wake up from our slumber and take positive action against the growing challenge of cyber-crime.

Conclusions and suggestions

Cyber jurisdiction is still in the nascent stage of development in law and a lot needs to be done fast in this area. Due to manifold increase in economic and other activities in the cyber world, at times illegal in nature, impacting almost every country in the real world, cyber jurisdictional issues need to be sorted out in national laws as well as uniformity in laws need to be brought about in such cases, and more importantly, not let the cyber criminals go unpunished due to gaping loopholes in existing laws or due to absence of laws altogether covering such matters both at the national as well as international levels.

Due to inadequacies in national laws, quite often ticklish legal situations arise in jurisdictional matters related to the Internet and the national laws are found wanting. Many times, case law has shown that for personal jurisdiction a Court requires that a defendant must provide more than mere accessibility to a Website or some sort of interaction should have been there. Whereas, the Web creator or information provider has to comply with the law of the State user is located and becomes subject of user's state jurisdiction and law.

Or in other words, from analysis of case laws, it may be concluded that a Website may be of three types, i.e., a passive Website, an active Website or where websites exchange information with a user interacted. A passive website is one that only makes information available to the Internet user and is not a sufficient ground for exercising cyber jurisdiction. Whereas, an active Website that enters into contracts and knowingly and repeatedly transmitted computer files would be properly subject to personal jurisdiction. However, in cases dealing with the middle ground, where interacted Websites exchange information with a user, the exercise of jurisdiction should be determined by examining the commercial nature of the exchange and the level of interactivity as interpreted by Courts.

Not only that, different States have adopted different laws covering personal jurisdiction and in the United States "Minnesota Warming" has been issued and similar unilateral declarations have been made by California and Texas. Incidentally, should India also resort to such a unilateral measure? Or for that matter should other states also do the same? Or would each state coming out with its own Internet Warning take care of the situation or would it lead to confounding the already complex situation, or more fundamentally, would this be the right way to go about sorting out the crucial issue of cyber jurisdiction? These questions

merit a separate analysis, which are not the subject of present inquiry.

Whereas, in India, Section 75 of the Information Technology Act, 2000 provides extraterritorial jurisdiction to the Indian Courts as often need to assume jurisdiction over foreign subjects would arise with increase in activity on the Internet. However, Section 75 has its own inadequacies and may not prove to be effective when it comes to its actual implementation. For instance, Section 75 appears to be ineffective on the ground that if an act is an offence or contravention under this Act and is committed by a person from outside India and which is affecting any computer or computer system or computer network in India and that act is not an offence in that country, then any judgment passed by an Indian Court may not be enforced by the Court of that foreign country because that foreign court may not accept the principal of extra territorial jurisdiction as given under Section 75 as that act in that country is not considered unlawful.[44]

More so, in such a situation, the international community has to take action due to the nature of the working of the Internet and its increasing use, specially exponential increase in international e-commerce activities and disappearance of geographical boundaries and conversion of the world into a global market, now seems to be the right time for international community to take immediate steps to formulate an international law relating to cyber jurisdiction. In this scenario, the United Nations should take a lead once again by not only encouraging member states to formulate national laws in this crucial area but also come out immediately with a model law to facilitate such a move and bring about uniformity in national laws covering cyber jurisdiction.

---

44 Kamath, Nandan. *Law Relating to Computers, Internet and E-Commerce*, op.cit., 2004, p.53.

References :

- Aswathappa, K. (2000): *Essentials of Business Environment*, Delhi: Himalayan Publishing House.
- Bakshi, Prashant (2000): "And Now Cyber Rouges" *In: The Login…In Tribune* (23 July), p. 12.
- Barula, Yogesh and Denzyl P. Dayal (2001): Cyber Crimes :*Notorious Aspects of the Humans and the Net, Vols*. 1-4, New Delhi: Dominant Publishers and Distributors.
- Johal, Navjit Singh (1998): "Address Social Issues in Framing Cyber Law" *In: The Tribune* (5 November), p.12.
- Kamath, Nandan (2000): *Law Relating to Computers, Internet, and E-Commerce: A Guide to Cyber Laws and the Information Technology Act, 2000*With Rules and Notifications, Second Edition, New Delhi: Universal Law Publishing Co.
- Mittal D.P. (2000): *Taxmann's Law of Information Technology (Cyber Law)*, New Delhi: Taxmann Allied Services Pvt. Ltd.
- Pati, Parthsastry (2001): "Cyber-Crime: Hardships to Curb it", *In the Lawyers Collective*, Vol. 16 No. 9 (September), pp. 26-27.
- Prasad, Satya T.V.R. (2001): *Law Relating to Information Technology (Cyber Laws)*, Hyderabad: Asia Law House.
- Subramanian, S. (1995): "Combating Computer Crime" *In: The Hindustan Times* (18 December) p. 12.
- Syed, Shakil Ahmad and Rajiv Reheja (2001): *A Guide to Information Technology* (Cyber Laws and E-Commerce), New Delhi: Capital Law House.
- Vishwanathan, Suresh T. (2001): *The Indian Cyber Laws*, New Delhi: Bharat Law House.