Chapter V

Judicial Response on Cyber Crime
CHAPTER-V

JUDICIAL RESPONSE ON CYBER CRIME

With the advent of the Internet, cyber law has become an emerging field. Cyber law encompasses cyber crime, electronic commerce, freedom of expression, intellectual property rights, jurisdiction and choice of law, and privacy rights. Cyber crime involves activities like credit card fraud, unauthorized access to computer systems, child pornography, software piracy and cyber stalking. Electronic commerce includes with encryption and data security. Freedom of expression includes defamation, obscenity issues and censorship. Intellectual property rights cover copyright, software licensing and trademark protection. Jurisdiction focuses on who makes and enforces the rules governing cyberspace. Privacy rights addresses data protection and privacy on the Internet.

There are many issues to be resolved in Cyber law. Two areas of cyber law requiring further clarification are cyber crime and jurisdiction. For example, in cyber law there are only a limited number of cases on point and no major statutory schemes on the books. Policy makers and attorneys dealing with cyber crime are often confined to referring to the imprecisely applicable and scarce existing statutes and cases\(^1\). In cyber jurisdiction, the Court must address the question of which lawmaker has jurisdiction over actions taking place on the Internet. In the few cases the Courts have adjudicated, they have applied long-arms statutes and personal jurisdictional principles in making decision. Due to the paucity of cyber jurisdiction cases, there is a limited amount of law for the legal practitioner for reference.

A. CYBER JURISDICTION:

The term ‘jurisdiction’ refers to the authority of a court to hear a case to resolve the dispute. In other words, court’s power to decide a case or issue a decree depends upon its jurisdiction. Since the legal environment of e-commerce has no geographical boundaries, cyber jurisdiction extends to all communications to anyone who has access to website.²

The law of cyber jurisdiction involves determination whether a particular activity in cyberspace is controlled by the laws of the State or country where website is located, or by the laws of the State where Internet Service Provider (ISP) is located, or by the laws of the State where user is located or by all these law?

The Internet can be seen as multi-jurisdictional because of the ease which a user can access a Web site anywhere in the world. It can even be viewed as a-jurisdictional in the sense that from the user’s perspective state and national borders are essentially transparent³. For courts determining jurisdiction, however, this situation is more problematic. The court in Zippo Manufacturing Co. v. Zippo Dot Com Inc.,⁴ said there is a global revolution looming on the horizon, and the development of the law in dealing with allowable scope of personal jurisdiction based on Internet use is in its infancy.

The developing law of jurisdiction must address whether a particular event in Cyberspace is controlled by the laws of the state of country where the Website is located, by the laws of the state or country

---

where the Internet service provider is located, by the laws of the state or
country where the user is located, or perhaps by all of these laws. A
number of commentators have voiced the notion that cyberspace should
be treated as a separate jurisdiction. In practice, this view has not been
supported by the Courts or addressed by the lawmakers.

Cyber jurisdiction issues have been dealt with primarily in the civil
courts. Since the advent of U.S. v. Thomas, and Minnesota v. Granite
Gate Resorts Inc, however, cyber jurisdiction issues have begun to be
examined in criminal courts as well.

(a) Cyber jurisdiction in Civil Cases:

In determining whether jurisdiction exists over a defendant, the
U.S. Federal courts apply the law of the forum state, subject to the limits
of the Due Process Clause of the Fourteenth Amendment.

In Bensusan Restaurant Corp. v. King, the plaintiff, operator
of the New York jazz club known as “The Blue Note”, complained that
the defendant had infringed on its rights by using its trademark.
Defendant, owner and operator of a small club called “The Blue Note”, in
Columbia, Missouri, had created a Web page, which allowed users to
order tickets to attend the club’s shows. The court had to decide whether
the creation of a Web site in Missouri containing a telephone number was
an offer to sell to citizens in New York.

5 Stuart Biegel, supra note 9, at 2.
6 David R. Johnson and David Post, Law and Borders—The Rise of Law in Cyberspace, 48
7 7.74 F. 3d 701 (6th Cir. 1996) (USA)
8 8.568 N.W. 2d 715 (Minn. App. 1997); aff’d 576N.W.2d 747 (Minn. 1998)
9 U.S.C. Const. Amendment. XIV
10 10.937 F. Supp. 295 (S.D.N.Y. 1996), aff’d, 126 F. 3d 25 (2d Cir. 1997)
The defendant argued the court lacked personal jurisdiction under New York’s long-arm statute. He defended all he had done was set up a web site in Missouri aimed at Missouri residents. Furthermore, any tickets sold over the Internet to users had to be picked up either at ticket outlets in Columbia, Missouri, or at the club on the night of the show.

The court agreed finding that it took several affirmative steps to obtain access to the Web site and use the information there. The court also ruled that there was no proof that the defendant had directed any infringing activity at New York. The court 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.

Under Due Process, in order for the court to exercise personal jurisdiction, it must be shown that the defendant had purposefully established minimum contact with the forum state such that the maintenance of the suit did not offend the traditional notions of fair play and substantial justice.11 The court ruled that the defendant’s simple creation of a Web site, that was available to any user who can find it on internet, was not an act of purposeful availment of the benefits of the state of New York. Creating a Web site was similar to placing a product into the stream of commerce. The Web site’s effect may be felt nationally or even internationally, but this without more, was not enough to establish an act was that purposefully directed towards the forum state. Based on these rulings the Court held that an exercise of personal jurisdiction would violate the protections of the Due Process Clause.12

12 Benususan, 937 F.Supp. at 301.
In *Inset Systems, Inc. v. Instruction Set, Inc.*\(^{13}\) the court held that advertising over the internet was purposefully directed toward the forum state\(^{14}\).

The US District Court for the Eastern District of Missouri reached a similar conclusion in *Martiz, Inc. v. Cyber Gold, Inc.*\(^{15}\), finding that it had jurisdiction over a California defendant in a trademark infringement case, where the defendant’s only contact with the state was through its California based website, which was accessible in Missouri\(^{16}\).

In *McDonough v. Fallon McElligott*,\(^{17}\) the court dismissed plaintiff’s contention stating that “because the web enables easy worldwide access, allowing computer interaction via the web to supply sufficient contact to establish jurisdiction would eviscerate the personal jurisdiction requirement as it exists. Thus, the fact that defendant has a web site used by Californians cannot establish jurisdiction by itself”\(^{18}\).

Similar decision is *Pres-Kap, Inc v. System one, Direct Access, Inc.*,\(^{19}\) which involved electronic contacts through a computerized airline reservation system. In *Burger King Corp. v. Rudezuitiz*,\(^{20}\) the US Supreme Court asserted jurisdiction on the grounds of accessibility of Internet. The court asserted that when a defendant has purposefully directed its activities to a forum state and caused injury to an individual

---

14. It is noteworthy that though a similar commercial situation was presented in Pres Kap, *Inc. v. System One*, Direct, but the court recognized the special nature of online transactions.
16. Supra Note 14
17. No. 95 Cir 4037 (S.D. Ca. August 15, 1996)
18. Supra note 14
20. 471US 462 (1985)
or entity, the state’s invocation of jurisdiction comports with its Due Process obligations\(^{21}\).

The same principle was carried forward in **Hearst Corp. v. Goldberge**,\(^{22}\) the court held that it lacked personal jurisdiction over the definition. In **Mo Mayo-San Francisco v. Charles Memminger**,\(^{23}\) it was held that simply registering someone else’s trademark as a domain name and posting a website on the Internet is not sufficient to subject a party domiciled in one state to jurisdiction in another. There must be “something more” to demonstrate that the defendant purposefully directed his activity in a substantial way toward the forum state.

The court in **Zippo Mfg. v. Zippo Dot Com. Inc.**,\(^{24}\) dealt with a cyber squatting case, where the plaintiff sued an Internet news service for trademark dilution, infringement and false designation for using the domain names “zippo.com,” “zippo.net”, and “zippo-news.com.” The court found jurisdiction and held that the likelihood of personal jurisdiction being found can be constitutionally based on an entity’s presence on the Internet. The court held that the extent of an entity’s presence, in the manner of sliding scale, was directly proportionate to the nature and quality of the commercial activity conducted over the Internet. The court found that a passive website that only made information available to interested users was not grounds for exercising jurisdiction. A 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 interactive websites exchanged information with a user, the exercise of jurisdiction


\(^{23}\)1998 us Dist Lexis 13154

should be determined by examining the commercial nature of the exchange and the level of interactivity.

(b) Cyber Jurisdiction in Criminal Cases:

The question of cyber jurisdiction in a criminal case came to the forefront of attention in early 1996 in **U.S. v. Thomas**, when the Sixth Circuit upheld the highly publicized conviction of a couple operating a pornographic bulletin board from their home. The defendants began operating the Amateur Action Computer Bulletin Board System (“AABBS”) from their home in Milpitas, California in February 1991. The AABBS contained approximately 14,000 Graphic Interchange Format (“GIF”) files. These files could be accessed by members who possessed the password. Once the password was entered, the users were able to select, retrieve, or download the GIF files to their own computers.

The government got involved in AABBS’ activities when a Web surfer found the site, explored the introductory screens, was offended and subsequently complained. In 1994, a U.S. Magistrate judge for the Northern District of California issued a search warrant authorizing a search of the defendant’s home. Because of the evidence found their computer system was confiscated.

The defendants were convicted in the U.S. District Court, Western District of Tennessee on federal obscenity charges. They appealed and the appellate court affirmed. There were two premises for their appeal: (1) The federal obscenity statute did not apply to intangible objects like computer GIF files, and (2) Congress did not intend to regulate the type of transmissions at issue because the federal obscenity statute did not expressly prohibit such conduct.

25.74 F.3d 701 (6th Cir. 1996)
The defendant asserted that the GIF files were an intangible string of 0’s and 1’s, which only became viewable images after being decoded in the AABBS member’s computer. The court disagreed, ruling that the fashion in which the images were transmitted did not affect their ability to be viewed or printed out by members in Tennessee. The defendant also argued that they were prosecuted under the wrong statute and that their conduct, if criminal at all, fell within the prohibitions of the statute which addresses commercial dial-a-porn operations. The court declined to accept this argument. Instead, it ruled that the statute must be construed to affect the intent of Congress, which was to prevent the channels of interstate commerce from being used to disseminate any obscene matter.

In Miller v. California, the court held that obscenity was to be judged by what the average person applying contemporary community standards would find to be obscene. 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 defendants asserted a more flexible definition was needed because BBS operators could not select who received their material.

The court ruled that the defendants had a pre-existing method of screening potential members. By pre-screening their members, they could protect themselves from being subjected to liability in jurisdiction with less tolerant standards. This could be accomplished by refusing to give passwords to users from those districts. The court further ruled the defendants were free to tailor their messages on a selective basis to the

communities it chose to serve. Accordingly, it was held by the court that there was no need to develop a new definition of community.

The case turned on the fact that even though the GIF files never actually left Northern California and were arguably not obscene under Northern California, Bay Area standards\(^{28}\), they were obscene by the standards of Memphis, Tennessee. The Court applied the community standards of the geographic area where the materials were sent as the proper test, in affirming the lower court’s holding that defendants were violating federal obscenity laws.

In *Minnesota v. Granite Gate Resorts Inc.*,\(^{29}\) the policy Minnesota’s Attorney General had stated in its Interest warning was tested in court. The 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 service as lawful on its Web page.\(^{30}\) The court denied the defendant’s motion to dismiss for lack of jurisdiction because of hits from Minnesota at the defendant’s Website, the availability of a toll-free number that users could call advertised on its Web page, and the number of Minnesota residents who had signed on to the defendant’s mailing list.

(c) **Cyber jurisdiction in International Cases:**

When adjudicating cases involving foreign nationals, the courts must balance several factors. On a case-by-case basis, the courts must consider the procedural and substantive policies of other countries whose interests are affected by the court’s assertion of jurisdiction. Keeping

---

28 In 1992 the AABBS computers were seized by the San Jose high-tech crime unit, scrutinized and found insufficiently offensive to warrant prosecution.
30 The advertisement on the Internet stated as follows: a. Wagernet “will provide sports fans with a legal way to Bet on sporting events from anywhere in the world… 24 Hours a Day!”
these policies in mind, the court must then consider the reasonableness of assertion of jurisdiction examined in the light of the interest of the federal government in its foreign relation policies. When extending jurisdiction into the international field great care and reserve must be exercised.\textsuperscript{31} Because of these sovereignty concerns, there is a higher jurisdictional barrier when litigating against a foreign national.\textsuperscript{32}

There are no international cyber jurisdiction cases, however, Asahi Metal Industry Company Case\textsuperscript{33} and Core-Vent Case\textsuperscript{34} can both provide the framework for future cyber jurisdiction cases.

The Supreme Court in \textbf{Asahi Metal Industry Company v. Superior Court},\textsuperscript{35} indicates that a plaintiff seeking to hale a foreign citizen into court in the United States must meet a higher jurisdictional threshold than is required when the defendant is a United States’ citizen. In Asahi the court found that even though Asahi had minimum contacts with the forum state, it would be unreasonable and unfair to find jurisdiction for three reasons: (1) the distance between defendant’s headquarters in Japan and the Superior Court of California and the unique burdens of submitting a dispute between two foreign nationals in a foreign legal system; (2) California’s and the foreign plaintiff’s slight interest in having the case heard in California; (3) the affect on the procedural and substantive interests of other nations by California’s assertion of jurisdiction over a foreign nationals.

\textsuperscript{32} Simatra v. national Enquirer, 854 F.2d at 1119.
\textsuperscript{34} Core-vent Corp. v. Nobel Industries AB., 11 F.3d 1482 (9th Cir. 1993)
\textsuperscript{35} 480 U.S. 102 (1987).
Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc. is an international civil case involving trademark infringement. In that case the court sidestepped the issue of international cyber jurisdiction relying on a previous 1981 injunction against the defendant to base its finding of jurisdiction. Nevertheless, the case provides useful insights into the application of cyber jurisdiction principals in international cases.

In order to support personal jurisdiction in cyberspace the courts now require that defendants provide more than mere accessibility to a Website. Some sort of interaction is required. A requirement, which may be satisfied as little as one contact. The trend appears to be that information providers must comply with the limitations of the laws wherever the user is located, or find themselves subject to the user’s state jurisdiction, and its civil and criminal laws. Case law indicates that the courts are inclined to expect the information provider to determine where the user is located and to block access to their site if access would be illegal in the user’s locale. If they own an 800 or 900 number, they could also be expected to block certain area codes to avoid prosecution.

B. Cyber jurisdiction in Information Technology Act, 2000

However, the law has gone much further. It shall also apply to any violation or contravention of the provisions of this Act done by any person anywhere in the world. By means of this provision, the law is assuming jurisdiction over violators of The Information Technology Act, 2000 outside the territorial boundaries of India. This provision is explained perhaps by the unique nature of cyberspace, which knows no boundaries.

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 India by any person irrespective of his nationality\textsuperscript{37}. It is however 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. \textsuperscript{38} The words “act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India” are very significant to determine jurisdiction of the IT Act over acts committed outside India. For assuming jurisdiction over an act constituting an offence or contravention under the IT Act, which is committed outside India, it has to be proved that the said act involves a computer, computer system or computer network located in India.

For instance, where a website is created in the US which contains pornographic material, it shall not give the IT Act jurisdiction to question the site unless the creation or maintenance or running of the site involves a computer, computer system or computer network located in India. But where the said website uses a server or any other computer network located in India, the IT Act would assume jurisdiction to question the website under section 67 of the IT Act.

Another instance to explain the jurisdiction of the IT Act is where a person from the US hacks a computer system or network in India, section 66 of the IT Act would come into play to punish the accused for hacking because his act involves a computer in India. Similarly, where a

\textsuperscript{37} Sec. 1(2) of IT Act, 2000
\textsuperscript{38} Sec. 75 of IT Act, 2000
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 to pay damages by way of compensation net exceeding Rs. 1 crore to the victim.

Section 75 of the IT Act is restricted only to those offences or contraventions provided therein and not to other offences under other laws such as the Indian Penal Code, 1860. Jurisdiction over other cyber crimes, for instance under the Indian Penal Code, 1860, has to be determined by the provisions of the Criminal Procedure Code, 1973. The fundamental principle on jurisdiction is the same under the IT Act\(^{39}\) and the Criminal Procedure Code, 1973, though stated differently. The basic legal principle of jurisdiction under the Code of Criminal Procedure, 1973 is that every offence shall ordinarily be inquired into and tried by a court within whose local jurisdiction it was committed.\(^{40}\) These principles in the Code of Criminal Procedure, 1973 apply for determining jurisdiction in trial by courts as well as in investigation by the police. In a case where an offence is committed in more places than one, or partly in one place and partly in another, or where it is continuing and continues to be committed in more than one local area, or where the offence consist of several acts done in different local areas, then it may be inquired into or tried by a court having jurisdiction over either of such areas\(^{41}\). In the event where it is uncertain in which of several areas the offence was committed, again it may be inquired into or tried by a court having jurisdiction over either of such areas of uncertainty.\(^{42}\)

---

\(^{39}\) Sec. 1(2) r/w Sec. 75 of IT Act, 2000
\(^{40}\) Sec. 177 of Cr. P.C., 1973
\(^{41}\) Sec. 178 of Cr. P.C., 1973
\(^{42}\) Sec. 178(a) of Cr. P.C., 1973
In a case where an act is an offence by reason of anything, which has been done and of a consequence, which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such act has been done or such consequence has ensued. For instance, in a case of defamation, either of the courts, i.e. of the place from where the defamatory letter was e-mailed and the place at which it was published or received, if different, shall have jurisdiction to inquire and try the same.

To cite another instance; where in pursuance of misrepresentation by A through e-mail from place X, property was delivered at place Y, A can be tried for the offence of cheating either at place X or Y. In a case where a person in Bombay does an act of hacking of a computer system located in Delhi, he may be tried either in Bombay or Delhi.

In a case where an act is an offence by reason of its relation to any other act which is also an offence or which would be an offence if the doer was capable of committing an offence, the first mentioned offence may be inquired into or tried by a court within whose local jurisdiction either of the acts was done. For instance, in a case of manufacture of sub-standard fertilizer in place X, which is marketed through e-commerce at place Y, prosecution can be launched at either of the said places because the marketing of the sub-standard fertilizers is an offence by reason of sub-standard manufacture.

Certain specified offences have been required by law to be inquired into or tried in certain places. For instance, an offence of criminal misappropriation or of criminal breach of trust, may be inquired into or tried by a court within whose local jurisdiction the offence was committed or any part of the property which is the subject of the offence

---

43. Sec. 179 of Cr. P.C., 1973
44. Sec. 180 of Cr. P.C., 1973
was received or retained or was required to be returned or accounted for, by the accused person\(^{45}\).

For example, if an employee of a company based at Delhi, by operating through the internet bank account of his employer company in a Bombay bank, transfers funds to his account at Calcutta, the case of misappropriation can be tried either at Delhi or Bombay where the offence was partially committed or at Calcutta where the money was received and retained.

The law also provides that in the case of any offence which includes cheating, if the deception is practiced by means of letters or telecommunication messages, it may be inquired into or tried by any court within whose jurisdiction such letters or messages were sent or where the same were received\(^{46}\). Moreover, any offence of cheating and dishonestly inducing delivery of property may be inquired into or tried by a court having jurisdiction on the place where the property was delivered by the person deceived or where it was received by the accused person\(^{47}\).

In a case where two or more courts take cognizance of the same offence and a question arises as to which of the courts has jurisdiction to inquire into or try that offence, this question shall be decided by the High Court, under whose jurisdiction both such courts function\(^ {48}\). However, if the courts are not subordinate to the same High Court, the question of jurisdiction shall be decided by the High Court within whose appellate criminal jurisdiction the proceedings were first commenced\(^ {49}\).

---

45. Sec. 181 of Cr. P.C., 1973  
46. Sec. 182 of Cr. P.C., 1973  
47. Sec. 182 of Cr. P.C., 1973  
48. Sec. 186 (a) of Cr. P.C., 1973  
49. Sec. 186 (b) of Cr. P.C., 1973
In such circumstances, all other proceedings with respect to that offence shall be discontinued. Where two or more courts have jurisdiction over an offence, the choice of the court for institution of the case lies with the complainant. He will obviously choose the forum, which is most convenient for him and most inconvenient for the accused.

The law of jurisdiction stated in the Criminal Procedure Code, 1973 and Section 75 of the IT Act, 2000, as discussed herein, is clear, specific and covers different situations which are likely to generally arise in cyber crime cases. The internet by its nature and purpose operates when the parties interacting or transacting are not physically face to face with one another.

Due to the global access of the internet, cyber crimes generally tend to transcend or disregard geographical boundaries. These factors imply that in most cases of cyber crime, except where insiders are involved, there would be two or more places, one from where the cyber criminal inflicts the injury—for instance hacks, and the place where the injury is inflicted—for instance at the location of the victim computer, which is hacked. This is in contrast to traditional crimes of rape, murder and kidnapping where the criminal and the victim are at the same place. Moreover, every criminal makes all possible attempts to conceal his identity and place of operation. Alibi is a common defence in criminal matters.

This basic tendency of a criminal coupled with the permissible anonymity provided by the internet makes the cyber criminal almost invisible. Thus, in terms of practical application of the law of jurisdiction over cyber crimes, in most cases, the place of jurisdiction shall be where
the victim is inflicted with the injury, whether personally, for instance by fraud, or on his computer, computer system or computer network.

There is a valid point in the criticism that such a law assuming extra territorial jurisdiction passed by the legislature is not enforceable in the real world. It is contrary to the principles of international law to assume jurisdiction over citizens of another country, and so, it is likely to lead to conflict of jurisdiction of different courts situated in different national jurisdictions. It is also important to note that there are differences between national legislation, laws, legal processes and procedures.

Further compounding the problem is the issue that a particular act in one national jurisdiction is legal and not barred by law but the same activity is illegal and barred by law, prevailing in another national jurisdiction. Another ground of criticism has been that Section 1 does not lay down the parameters of how such a provision would be enforceable in practical terms across transnational boundaries and jurisdictions. Governments can take recourse to the extradition process to bring to book the cyber criminals outside the territorial jurisdiction of their country, provided there is a valid extradition treaty in place between the relevant countries. But the route, as stipulated in Section 1 of the IT Act, 2000 is likely to throw up a complex arena of difficulties in actual day-to-day implementation.

The existing international law pertaining to sovereignty of a nation also details that a sovereign nation can make laws affecting people who reside within its territorial boundaries. However, the birth of Internet has seen geography become history and transactions taking place over networks are transnational in nature, thereby complicating the entire issue
of jurisdiction. This becomes all the more evident from the emerging principles from various judgments relating to Jurisdiction over Internet. From the beginning of Internet, the issue of jurisdiction has continued to challenge legal minds, societies and nations in the context of the peculiarly inherent character of the Internet. Section 1(2) and Section 75 of the IT Act, 2000 provide for extra-territorial jurisdiction of the Indian courts, which, however, seem implausible to be implanted. The courts in India at present have not been uniform in following the US trend of asserting jurisdiction on the basis of active accessibility of site. So far, in various Internet domain names related cases, the Delhi High Court has assumed jurisdiction merely on the basis of accessibility of Internet.

Judicial Trends in India:

It must be stated that Indian case law on cyber jurisdiction of the courts was almost non-existent until the Information Technology Act, 2000 was enacted and enforced on October 17, 2000. The development of information technology as a faster and quicker means of communication in the new millennium has led to certain unforeseen consequences resulting in cybercrimes coming before the Courts for adjudication.

The case of P.R. Transport Agneey v. Union of India and others,\(^\text{50}\) involved the question of jurisdiction of court where the contract between the parties residing in different places has been made on e-mail. In this case, Bharat Cooking Coal Ltd. (BCCL) held an e-auction for coal in different lots in which plaintiff’s (P.R. Transport agency) bid for 40000 metric tons of coal from Dobari colliery was accepted. The BCCL communicated the acceptance of bid by e-mail on July, 19, 2005. In

\(^{50}\) AIR 2006 All 23 (decided on 24.9.2006).
response, the plaintiff deposited the amount of 81.12 lakhs through a cheque in favour of BCCL which accepted the cheque and encashed it but did not deliver the coal to the plaintiff. Instead, it (BCCL) informed the plaintiff through e-mail communication that the said e-auction stands cancelled “due to some technical and unavoidable reasons”. The plaintiff found that the e-auction of sale of coal was cancelled by BCCL as there was some other person whose bid for the same was higher, which had not been considered earlier due to some flaw in the computer or its program or feeding of data.

The plaintiff (P.R. Transport) challenged the validity of cancellation of its contract by the defendant in the High Court of Allahabad. The defendant (BCCL) objected the territorial jurisdiction of the Court on the ground that the High Court of Allahabad had no jurisdiction in the case as the cause of action had not arisen in the state of Uttar Pradesh. The plaintiffs, on their part, argued that the case fell within the jurisdiction of the Court because the communication of acceptance of the tender was received by them through e-mail in Chandauli in U.P. Having heard both the parties, the High court held that in case of e-mail acceptance, the data transmitted from anywhere by the account-holder goes to the memory of ‘server’, which may be located anywhere and can be retrieved by the addressee account-holder from anywhere in the world. Therefore, there is no fixed point either for transmission or for receipt of e-mail. As provided in Section 13 (3) of the Information Technology Act, 2000, “an electronic document is demand to be received at the place where the addressee has his place of business.

The acceptance of the tender will be deemed to be received by the plaintiff (P.R. Transport) at the place where it has place of business i.e. Varanasi and Chandauli, both in the state of Uttar Pradesh, hence the
Allahabad High Court had the jurisdiction to decide the case. On the basis of decision in this case, it may be concluded that the judicial trend with regard to exercise of jurisdiction by courts in cybercrimes must conform to the norms of fair play and justice, which invariably depend on following considerations:

(a) the extent of purposeful intrusion or illegal activities affecting State’s affairs;

(b) extent of conflict with sovereignty of the State;

(c) the forum of State’s interest in adjudication of the dispute;

(d) state's responsibility for protecting the interests of parties providing them relief; and

(e) existence of an alternative forum.

In order to support State’s jurisdiction in cyberspace, the law requires that it not only provides accessibility to website but also in some way interacts with the victim.

C. Judicial Response to combat Cyber Crimes:

The internet culture in its wake has give rise to a number of online disputes, differences, and controversies etc. resulting out of misuse of abuse of computer networks for illegal activities. Though disputes as such are not new to human society as they are known to have existed ever since the dawn of human civilization, but the distressing factor is that disputes relating to online transactions are entirely diverse in their nature, scope and treatment and therefore, the resolution of these cyber-related disputes has emerged as a serious challenge for the courts of law because
of the details involved in them with which the Judges are not thoroughly conversant.

The factors which hamper judicial sentencing in cybercrime cases are as follows:

i. Global nature of these crimes is such that they do not recognize geographical or territorial boundaries;

ii. Want of clarity as to which court would have the exclusive jurisdiction to try the case;

iii. Variations in the legal systems and laws and procedure of different countries as regard admissibility of cyber-related cases; and

iv. Uncertainty as to the exact definition of cybercrime and activities which can be included within the ambit of ‘cybercrime’.

Cybercrime being of an intangible nature, it does not require any physical violence or the presence of accused at the scene of crime. Under these circumstances, the traditional adversarial system of litigation would hardly meet the ends of justice in cases relating cybercrime.

Commenting on the problem faced by the judiciary and the enforcement agencies in dealing with computer-related crimes, the Supreme Court of India in State of Punjab and Others v. M/s Amritsar Beverages Ltd. and others, 51 observed,

“Internet and other information technologies have brought with them the issues which were not foreseen by law. It also did not foresee the difficulties which may be faced by the officers who may not have any scientific expertise or not have the sufficient insight to tackle with the

51 AIR 2006 SC 2820 (Para II).
new situations. Various new developments leading to various kinds of crimes unforeseen by our Legislature came to immediate focus. Information Technology Act, 2000, although was amended to include various types of cybercrimes and the punishment for them, does not deal with all problems which are faced by the officers enforcing the Act.”

A cursory glance at the judicial administration in the Indian setting would disclose that the factors which influence judicial sentencing by and large include age, sex, educational background, mental frame and maturity of the offender. His motive and the circumstances under which the offence was committed and its consequence on the victim or the society also has a bearing on the sentencing of the accused.

The offender’s young age, immaturity and previous clean record are generally good reason for leniency in sentencing while recidivism, persistent association with criminals or criminal world as also the gravity or seriousness of the crime, attracts severe punishment. However, these are mere generalizations and do not in any way bind judicial discretion in sentencing the criminals. The Judges while considering the punishment can hardly afford to overlook the overall collision of crime on society as a whole. Court’s decisions therefore, play a very important role in deciding a future course of action in related cases52.

Although the case law available on cybercrime is far scantier as compared with the traditional crimes, it is constantly growing due to computer becoming more and more user-friendly with the people. The courts have generally shown a tendency to treat cyber criminals guilty of premeditated crime as probable danger to society and therefore, they are unenthusiastic in mitigating the sentence of such offenders.

52. Paranjape N.V.: Criminology and Penology (13th ed.) page 246-47
Some international and national judicial responses on cybercrime have been given below to put in the legal perspective of the issue.

a. Judicial Response to Curb Pornography:

Pornography is the depiction of the obscene and indecent either literally or pictorially, which has the tendency to pollute the minds of the children and has every potential to adversely affect the moral hygiene of the society and, therefore, the law strictly prohibits the creation, publication and circulation of the same in the society to preserve the moral fabric of the society. Publishing the pornographic material, therefore, it becomes urgent that the malaise of the same should be checked Computer and internet are the easiest methods of circulating and Generation, publication and circulation.

Pornography has been defined in the Oxford Dictionary as “The explicit description or exhibition of sexual subjects or activity in literature, painting, films etc., in a manner intended to stimulate erotic rather than aesthetic feelings; literature etc. containing this.”

The crime called cyber pornography presents itself in various ways posing new and new challenges before law and Courts both. Thus it will be beneficial to look in to some decisions of Courts in order to appreciate the functioning of law vis-à-vis the incidents of cyber pornography.

In United States v. Thomas, a federal postal inspector in Tennessee (U.S.A.) downloaded pornographic materials from the site of a Bulletin Board Service (BBS) operator in California. He was arrested and

55 74 F. 3d 701 (6th Cir. 1996) (USA)
convicted for delivering pornographic material which is an offence under federal obscenity laws. The court laid down certain important principles of law. It was held that GIF files are not “intangible” for the purpose of federal obscenity laws. The distribution of obscene materials would fall within the expression of ‘knowing even without defendants having specific knowledge of each individual transmission’.

Further, obscenity is to be measured by “community standards” of the place where material is received. The defendant’s ability to control subscription and access to their BBS made them liable in this case for the downloading that occurred in Tennessee and thus amenable to jurisdiction there.  

In an American case, namely, United States v. Kufrovich, the accused was charged of an offence under Section, 2422 (b) and 2433 (b) of the US Criminal Law for using internet communication to knowingly persuade a minor to engage in sexual activity with him. The accused argued in his defence that his contact with the victim was only through the internet and not direct, hence he was constitutionally protected under the First Amendment and the conversation through the internet could not be used against him in evidence. The Court, however rejected the defence and held that the Communications Decency Act under which the charges were brought against the accused, criminalises the use of internet and telephone lines for the purpose of attracting a minor into sexual activity.

In R v. Graham Waddon, Southwark, the defendant had created images which were illegal under UK law, and had made the same available to subscribers on a series of sites based in US and hosted by a

---

58 A decision by the Crown’s court, dated 30 June, 1999
US based Internet Service Provider (ISP). When charged of publishing obscene articles contrary to S. 2(1) of UK’s Obscene Publications Act, 1959, the defendant claimed that since he had published the said porn literature abroad, the UK law did not apply to his act and, therefore, a UK Court had no jurisdiction in his regard.

The Court, however, did not accept either of the pleas forwarded by the defendant. The Court observed that, under section 1 (3) (b) of the Obscene publications Act, 1959, publishing included data stored electronically and transmitted. Since to transmit meant to send from one place or person to be other, in the instant case, the act of publication took place as soon as the defendant transmitted the data to the service provider; and the publication or transmission also took place while the data was received. In case of the viewers from UK, the sending and receiving both took place in UK, that is, within the jurisdiction of the Court; and it was irrelevant that ‘the transmission may have left the jurisdiction (for some time) between the sending and receiving’. Arguing thus the Court held that it had the jurisdiction to prosecute the accused for pornography.

According to the facts of the case, the defendant had created pornographic images, which were illegal under the UK’s Obscene Publications Act. He ran a series of sites based in the US, hosting them on a US based Internet service provider. These images were accessible to anyone in the world via the Internet who became a subscriber by giving credit cards details. He was charging UK customers 25 pounds a month for access. The subscriber was given a password and could log onto the various websites to obtain the images.59

i. Judicial response before the IT Act 2000 in India:

Sukanto Haldar v. State of West Bengal\textsuperscript{60} case were relating to magazine “Nara Nari” which was treated as obscene publication. Therefore, to give effect to public morality above art, literature the court under s. 292 of the Indian Penal Code 1860 convicted the petitioner and sentenced him to two months rigorous imprisonment and fine of Rs. 200 in default to rigorous imprisonment for two weeks.\textsuperscript{61}

Shaw v. Director of Public Prosecution\textsuperscript{62} in the UK was related to a magazine named “The Ladies Directory” to distribute in market which contained names, addresses of prostitutes, pornographic photographs and the descriptions of their practices. The accused was charged for such pornographic distribution in public as an offence because it corrupts the mind of people or individuals and this act was treated by court as ‘a conspiracy to corrupt public morality’. The judiciary referred here –

(i) John Staurt mills principle of ‘harm to others’ mentioned in his book “On liberty”;

(ii) The conclusion of the debate of H.L.A. Hart and Prof. Devline about enforcement of morality by law where they concluded with the need of the balance between law and morals and shared morality; and

(iii) The recommendations of the Wolfenden Committee’s in the year 1957 in the UK which was similar to J.S. Mills principle.

(iv) The Wolfenden Committee’s recommendations were that while prostitute and homosexual parties are two consenting adults and doing something within four walls without hampering others or

\textsuperscript{60} AIR 1952 Cal 214.
\textsuperscript{62} (1961)2 ALL ER 44 B.
without causing harm to others, the State shall not enter into individual’s private liberty and the same activities will not be treated as a crime.

Indian judiciary whole heartedly followed these principles as well as Hiclin Test and decision of the U.S. Court in Roth’s case. In Ranjit D. Udeshi v. State of Maharashtra, the Supreme Court of India declared “Lady Chatterley’s Lovers” written by D.H. Lawrence as obscene book and publication. The Court held that there is difference between ‘obscenity’ and ‘pornography’. Precise definitions are not possible. However, obscenity is any material, which tends to corrupt, cause annoyance, something of horror, indecent, immoral or with sexual tendency. “Pornography” means any material in writing, picture or other form, which is intended to arouse sexual desire. Both are against public morality and decency.

Legislation which prohibits ‘obscenity’ and ‘pornography’ are laws with moral value and when there is synthesis between law and morality, the situation will be balanced with shared morality.

ii. Judicial response in India after the Information Technology Act, 2000:

In Jayesh S. Thakkar v. State of Maharashtra, on 29th July may 2001, the petitioners wrote a letter to the Chief Justice of the Bombay high Court. The complain of the letter was about pornographic websites on the internet. The letter was treated as *suo motu* writ petition.

---

63 AIR 1965 SC 881; (1965)2 Cr LJ 8.  
On 26th September 2001, the Division Bench of the Bombay High Court consisting of B.P. Singh, CJ and Dr. D.Y. Chandrachurd, J.; and passed an order to appoint a committee to suggest and recommended ways of preventive and controlling measure and means to protect children from access to pornographic and obscene material on the internet.

The committee considered several public opinions through internet and other media and recommended in a report. The Bombay high Court Special Committee’s report on Shielding Minors from Cyber porn i.e., Protecting Minors from Unsuitable Internet Material on 30th January 2002 was as follows:

(1) Site Blocking: The committee comprehensively rejected the proposal for site blocking as being technically and legally unsound.

(2) Cyber Cafes: the Committee’s recommendations include:

   (a) A suggested definition of cyber cafes to be included in the rules under the Bombay Police Act.

   (b) Procedures for licensing cyber fares as none are as yet licenced or regulated.

   (c) Regulations requiring cyber café operators to demand photo identity cards of any kind from all users.

   (d) Requiring that minors be restricted to using machines in the common open space of cyber cafes i.e., not in cubicles.

   (e) Requiring that these machines be fitted with software filters.
(f) Providing for the maintenance of internet protocol address allocation time-stamped logs for all machines in the cyber café network.

(3) Service Providers: The recommendations cover

(a) requirements for maintenance of time-stamped logs of different descriptions;

(b) requirements for synchronization of internal clocks and connectivity authentication logs.

(4) Educational Measures: These include

(a) Electronic mail and website information to be provided by internet service providers informing the public about hazards and possible solutions.

(b) Offering filters software to subscribers as an option.

(c) Setting up a hotline to the cyber crime investigation cell.

(d) Taking steps to increase awareness about cyber crime in general.

As regards the reported Indian cases on cyber pornography, they are far and few as most of them are disposed of in the lower Court at the magisterial level. However, the case of State of Tamil Nadu v. Suhas Katti,66 deserves a special mention in this context since it was disposed of within a record period of seven months from the date of filing of the FIR. The credit for expeditious investigation of the case goes to the Chennai Cyber Crime Cell which produced 18 witnesses and 34


{304}
documents in support of the prosecution case. The facts of the case were as follows.

The accused Suhas Katti was sending obscene, defamatory and annoying messages about the complainant, a divorce woman on e-mails and in the Yahoo Message group. He had opened a false e-mail account in the name of the victim. The e-mails carried a message that the victim lady was soliciting and therefore, she was receiving annoying phone calls from callers to have sex. She filed FIR against the unknown accused in the Cyber Crime Cell, Chennai. The police investigation revealed that the accused was a known family friend of the victim who was residing in Mumbai and was interested in marrying her. She, however, married another person whom she divorced after sometime, so the accused again started contacting her for marriage with him, to which she declined. Thereupon, he started harassing her by sending obscene and defamatory e-mails.

The accused was charged under Section 67 of the I.T. Act, 2000 read with Sections 469 and 509 of the Indian Penal Code. He pleaded that the offensive e-mails might have been sent to the complainant (lady) either by her ex-husband whom she had divorced or she might have herself managed to do so in order to implicate the accused because he had turned down her request to marry her. It was also argued on behalf of the accused that documentary evidence against him were not sustainable under Section 65(b) of the Indian Evidence Act. The Court, however, relied upon the expert witnesses and other evidence before it including the witnesses of cyber café owner and convicted the accused for the offence under Sections 469/509; IPC and Section 67 of the I.T. Act.
The accused was sentenced to undergo rigorous imprisonment for 2 years and to pay a fine of Rs. 4500/- for the offence under Section 469, and imprisonment for one year with a fine of Rs. 500/- for the offence under Section 509 of IPC, and a sentence to undergo simple imprisonment of 2 years and a fine of Rs. 4000/- for an offence under Section 67 of the Information Technology Act. All the sentences were to run concurrently.

In *Fatima Riswana v. State Represented by ACP, Chennai and other*, 67 the appellant was a prosecution witness wherein respondents 2 to 6 were accused facing trial for the offence of cyber pornography under Section 67 of the Information Technology Act, 2000 read with Section 6 of the Indecent Representation of Woman (Prohibition) Act, 1986 and Section 5 and 6 of the Immoral Traffic (Prevention) Act, 1956 as also under Section 27 of Arms Act, 1959 and Sections 120-B, 506(ii), 366, 306 and 375, IPC. The accused named Dr. L. Prakash allegedly exploited certain men and women for the purpose of making pornographic photos and videos in various acts of sexual intercourse and selling them to foreign websites. The case was tried by Vth Fast Track Court, Chennai which was presided over by a lady Judge as that Court happened to be a ‘Mahila Court’ constituted by the Government of Tamil Nadu for speedy trial of cases of offences committed against women.

While the trial was pending before the said Fast Track Court, the accused filed revision petition against the Court order rejecting their demand of supply of copies of 74 compact discs (CDs) containing alleged pornographic material. The revision petition was rejected by

---

Madras High Court holding supplying such a large number of copies of CDs was not possible as it may give room for copying such illegal material for further circulation. The Court, however, permitted the accused persons to peruse the CDs in the chamber of the Presiding Judge in the presence of their advocates, the expert and public prosecutor.

The Public Prosecutor and the petitioner’s Counsel submitted that it would be embarrassing for them to view the said CDs in the presence of learned District Judge who was a lady Judge. The High Court observed that since the accused had not filed any application for transfer of the said case to some male Judge, it was for the Presiding Lady Judge to choose whether she wanted to try to case herself or get it transferred to a male Judge colleague. The High Court, however, transferred the case to Fast Track Court IV which was presided by a male Judge as requested by the Public Prosecutor but without hearing the petitioner.

The appellant, therefore, moved a criminal revision in 2004 contending that the transfer of the case from lady Judge to male Judge would embarrass the appellant, she being woman. It was also contended that such transfer was contrary to the object creating Mahila Courts, as also the earlier decision of the Apex Court. The High Court rejected the appeal and therefore, the appellant went in appeal before the Supreme Court.

The Apex Court held that the entire approach of the High Court in the instant case was against the interest of the witnesses who were really the victims in the case. The Court further observed that since the Presiding Lady Judge had not expressed any embarrassment, it was unreasonable to presume that it would cause here embarrassment, more so when she had not expressed any desire that the case be transferred to
some male Judge. Allowing the appeal, the Apex Court held that the High Court should not have interfered in the matter.

The Additional District Court and Sessions Court here was upheld a lower court’s verdict in the first cyber case State v. Ts. Balan and Aneesh Balan filed in the State sentencing a Pentecostal Church priest and his son to rigorous imprisonment in 2006.

Disposing of the appeal filed by the priest T.S. Balan and his son, Aneesh Balan, against the order of the Chief Judicial Magistrate. Additional District Judge T.U. Mathewkutty said it was time the government took effective measures to check the growing trend of cyber crimes in the state. The court upheld the magistrate’s order sentencing the two to three-year rigorous imprisonments and imposing a fine of Rs. 25,000 under section 67 of the Information Technology Act; awarding six months rigorous imprisonment under section 120(B) of the Indian Penal Code; and ordering one year rigorous imprisonment and imposing a fine of Rs. 10,000 under section 469 of the code. The court revoked the sentence under Section 66 of the IT Act. The cyber case dates back to January-February 2002 and the priest and his son became the first to be convicted of committing a cyber crime.

The two were found guilty of morphing, web-hosting and e-mailing nude pictures of Pastor Abraham and his family. Balan had worked with the pastor until he fell out with him and was shown the door by the latter. Balan joined the Sharon Pentecostal later. The prosecution said the duo had morphed photographs of Abraham, his son, Valsan Abraham, and daughter, Starla Luke, and e-mailed them from fake mail IDs with captions. The morphed pictures were put on the web and the

---

68 Additional District and Session Court, Kerala, 2006.
accused, who edited a local magazine called ‘The Defender’, wrote about these photos in his publication.

Valsan received the pictures on the Internet and asked his father to file a complaint to the police. A police party raided the house of Balan and his son at Perumbavoor and collected evidences. The magistrate’s verdict came after a four-year trial, for which the court had to procure a computer with Internet connection and accessories. The police had to secure the services of a computer analyst too to piece together the evidence. Twenty-nine witnesses, including the internet service provider and Bharat Sanchar Nigam Ltd., had to depose before the court.

b. Judicial Response on Child Pornography:

Child pornography refers to images or films (also known as child abuse images) and in some cases writing, depicting sexually explicit activities involving a child; as such, child pornography is a record of child sexual abuse. Under the IT Act, 2000 as amended by the ITAA, 2008, crime of Child Pornography under 67-B says, whoever publishes or transmits or causes to be publishes or transmitted material in electronic form which depicts children engaged in sexually explicit act or conduct or creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or facilitates abusing children online or records in any electronic form own abuse or that of others pertaining to sexually explicit act with children is known as child pornography.
In United States v. Crandon,\textsuperscript{69} Richard Crandon pleaded guilty before the Court for receiving child pornography. His crime was much more than just downloading the illicit material from the internet. Crandon met a fourteen year old girl online and ultimately meeting with her to have sexual relations and took the photographs of that intercourse. Crandon and the girls used to frequently interact over the telephone and used to discuss about their future prospects. The girl wanted to go to New Jersey from Minnesota along with Crandon. They went about materializing their plan and left for New Jersey form Minnesota. On their way they came to know that the authorities were looking for them. The girl was sent from Minnesota. Crandon contested the deprivation of his access to the Internet during the period of his imprisonment on the ground that the Court has to seek the prior approval from the probation officer. Further he pleaded that the non accessibility would hinder his employment and the business wince computers and the internet are inextricably tied. Court upheld that the restrictions was tenable in the light of the first amendment which related to the protecting the interest of the public.

In United States v. Hockings,\textsuperscript{70} it was held that the computer graphic interchange files (GIFs) in binary format fall within the definition of visual depictions. The fact that such files require the use of personal computers, hardware and software to depict images of child pornography does not put them outside the statute.

A U.S. court in United States v. Simpson,\textsuperscript{71} laid down that the detectives affidavit describing aborted transaction negotiated in Internet

\textsuperscript{69} 494 U.S 152 (1990)  
\textsuperscript{70} 129 F. 3D 1069 (9th cir. 1997) U.S.A.  
\textsuperscript{71} 152 F. 3d 1241 ( 10th cir. 1998) U.S.A.
chat room to exchange child pornography was sufficient to constitute portable cause in obtaining search warrant.

The U.S. District Court of Maryland in United States v. Mathews, held that each transfer by e-mail of a child pornography image is a separate offence under federal law. The defendant’s argument was rejected by the court who had contended that the successive e-mail transmission were all part of a single online “conversation”. The defendant’s defence that he was involved in investigative journalism was also rejected by the court.

In United State v. Gray, the court held that child pornography discovered during a search conducted pursuant to obtaining a warrant for materials related to computer tampering was admissible. Defendant argued that files with the .JPG extension were presumptively pictures and not related to subject of search. Court noted that hackers frequently mislabel files, and FBI agents were not required to take file names at face value.

In State of New York v. BuffNet, an Internet service provider (ISP) pled guilty to the misdemeanor charge of knowingly providing access to child pornography. A two-year investigation found that ISP, BuffNet, knowingly hosted a child pornography newsgroup called “Pedo University”. The police notified BuffNet that they were hosting illegal content, yet BuffNet failed to remove the newsgroup from its servers. Police then seized the ISP’s servers. Buffnet was levied a $5000 fine, and removed the obscene content.

---

73 78 F. supp.2d 524 (E.D. Va.1999) U.S.A.
74 New York Appellate Division, Fourth Judicial Department (2001) (USA)
In **U.S. v. Jesus Norberto Evans-Martinez**, the defendant was convicted for sending emails advertising the creation of a Yahoo! Group for sharing child pornography.

Also, in **Jeffrey L. Cashatt v. State**, the Court of Appeal of Florida affirmed conviction against the defendant, who knowingly used a computer on-line service, Internet service or local bulletin board service to seduce, solicit, lure, or entice a child or a person believed to be a child, or attempt to do so, in violation of section 847.0135(3), Florida Statutes.

The **Airforce Bal Bharti School Case** was filed in the Juvenile court, Delhi on the charge of cyber pornography. Some jurists say this is the first Indian cyber pornographic case which was charge sheeted in the juvenile court. The brief facts in issue were that a student of the Airforce Bal Bharti School, Lodhi Road, New Delhi was arrested by the Delhi Police in the year 2001 April.

The alleged accused was then a class XII student who created a pornographic website as revenge of being teased by classmates and teachers. He listed in that website the name of his 12 schoolmates’ girls and teachers in sexually explicit manner. He was then suspended by the School Authorities though the juvenile court allowed his bail prayer. However, he was charged under s. 67 of the Information Technology Act 2000, and ss. 292, 293, 294 of the Indian Penal Code and the Indecent Representation of Women Act. The most significant steps were taken by the law enforcement agencies in India.
In another case, a **Swiss Couple**\(^{78}\) in Mumbai would gather slum children and then force them to appear for nude and obscene pornography. They would then upload these photographs to websites specially designed for pedophiles. The Mumbai Police arrested the couple for pornography and charged them for the offence of cyber pornography under Section 67 of the I.T. Act read with Section 292 and 509, IPC. But they were later let off for want of sufficient evidence against them.

In the case of **Avnish Bajaj v. State (NCT Delhi)**,\(^{79}\) Baazee.com was an online auction website and Avnish Bajaj was in Chief Executive Officer (CEO). He was arrested in December, 2004 for distributing cyber pornographic material. The charges against him arose from the fact that someone had sold copies of pornographic CD through Baazee.com website. The CD was also being sold in the Delhi market. It was as a result of joint action of Delhi and Mumbai police that the accused was arrested. However, he was later released on bail by the Delhi High Court as there was no prima facie evidence that Mr. Bajaj directly or indirectly published the said pornography and the actual obscene recording of chip could not be viewed on Baazee.com. The investigation in this case revealed that Bajaj was of an Indian origin and had family ties in India. His company’s web-site i.e. Baazee.com was a customer web-site which was dealing online sale of property on commission basis. An obscene MMS clipping ‘A DPS girl having fun’ was listed for sale on Baazee.com on November 27, 2004 and some copies of this clipping were sold by the company.

---

\(^{78}\) Swiss couple cyber pornography case, Mumbai 2003
\(^{79}\) (2005) 3 Comp. LJ 364 (Delhi). This case is popularly known as Baazee.com case.
The accused Mr. Bajaj in his defence pleaded that Section 67 of the Information Technology Act under which he was charged and arrested relates to publication of obscene material and not the transmission of such material. Moreover, having come to know about the illegal character of the disputed CD, he initiated steps to immediately stop the sale within 38 hours since the intervening period was a weekend. He further contended that the said obscene clip could not be viewed on the portal of Baazee.com and the sale proceeds were not routed through him.

The question for decision before the Court in this case was to draw a distinction between internet service provider (ISP) and content provider. The Court ruled that the burden rests on the accused to prove that he was only the service provider and not the content provider. The court held that accused deserved to be released on bails as the evidence showed that the obscene material may have been unwittingly offered for sale on his company’s web-site and there was probability of the alleged crime having been actually committed by some other person. The accused was, however, ordered to furnish two sureties of one lakh rupees each and surrender his passport and not to leave India without the permission of the Court. He was finally enlarged on bail subject to condition that he shall participate and assist in the investigation.

In Hari Ram v. State of Rajasthan & Another,80 it has been observed that “the law as now crystallized on a conjoint reading of Sections 2(k), 2(l), 7A, 20 and 49 read with Rules 12 and 98, places beyond all doubt that all persons who were below the age of 18 years on the date of the commission of the offences even prior to 1st April, 2001, would be treated as juvenility was raised after they had attained the age

---

80 Criminal Appeal No. 907 of 2009 (Arising out of S.L.P. (Crl.) No.3336 of 2006).
of 18 years on or before the date of commencement of the Act and were undergoing sentence upon being convicted.”

c. **Judicial Response on Online Fraud:**

The term “Internet Fraud” is very comprehensive but has not been specifically defined under the IT Act. This term will possibly include other crimes also which have been expressly defined in the IT Act. The frauds through Internet Frauds will take a variety of forms and their classification cannot be easily maintained. The courts in America are busy to resolve Internet frauds

**United States v. Morris**[^81] is one of the landmark case in the USA which deals with cyber fraud. Morris, the accused was held guilty of violating Title 18 U.S.C.s. 1030(a)(5)(a) by the Jury in trial. Morris was authorised to use computers at Cornell, Harvard and Berkeley. He was authorised to communicate through internet to other computers, computer system and network. He was authorised to send e-mail, collect informations etc. He transmitted “worm” which was considered as exceeding authorised access or unauthorised access. He used send e-mail and connect other computer and by this way unauthorisedly accessed other computers in fact, he found holes in programmes which gave scope to him for a special and unauthorised access route into others computer. He was sentenced to 3 years of probation, 400 hours of community service and fined with $ 10,050. He appealed to the Circuit Court against the decision of the trial court. Section 1030(a)(5)(a) of the Computer Fraud and Abuse Act 1986 provides that whoever knowingly causes the transmission of a programme, information, code or command and as a result of such conduct, intentionally cause damage without authorization

[^81]: 928 r. 2d 505 (2nd cir), Cir Court denied, 502 U.S>817 (1991).
to a protected computer be punished. Morris contended that his conduct was almost exceeding authorised access. And the evidence was also not sufficient to convict him of unauthorised access. The Circuit Judge Newman affirmed the District Courts’ judgment.

In the context of on-line cyber frauds, the notorious **World Wide Nigerian Scam**\(^2\) deserves a special mention. The scam, better known as Advance Fee Fund (AFF) Nigerian Fraud or the ‘419 Fraud’ named after Section 419 of the Criminal Court of the Nigeria, which is operating in most of the European and Anglo-American countries since 1980’s has duped the business world to the tune of Billions of US dollars. It is reported to be the fifth largest industry in Nigeria operated by unscrupulous business elites under the successive Government of that country. The *modus operandi* of the scam is as follows:

The victim receives an unsolicited fax, e-mail or letter concerning Nigeria or any other African nation, mostly from West Africa such as Ghana, Togo, Liberia, Sierra, Leone, Ivory Coast etc; requesting for legal and legitimate business proposal or service contracts. The victim is asked to pay an advance fee of some kind which may be in the form of ‘transfer tax’, ‘performance bond’ or for credit privileges. Once the victim pays the fee, many more requests for advance payments on one pretext or another come to the victim until he either decides to quit or runs out of money, or both.

Alarmed by the widespread Nigerian “419 Fraud’ the Government of USA, UK, Canada, South Africa etc. have warned the business community to be alert and not to respond to 419 letters, instead file a complaint against the sender with the national law enforcement agency as

\(^2\) US Department of State of International Narcotics and Law Enforcement Affairs (April, 1997).
also Nigerian Embassy and the Central Bank of Nigeria. Those who have fallen a pray to such scam may also file a complaint with the Nigerian Economic and Financial Crimes Commission. In Canada, the regional offices of the Commercial Crime Branch may be contracted for redressal and relief. In UK, those effected or cheated by the 419 Advance Fee Fund Nigerian Scam may forward their complaint to local fraud squad for investigating quoting ‘NCIS’ (Western African Organised Crime Section) in the correspondence. Under no circumstances reply should be sent to the fraud operators. Anyone outside the UK may also seek help and advice from UK in case he received a 419 letter or falls a victim to 419 fraud.83

In FTC v. Craig Lee Hare,84 the action was for deceptive trade practices arising from on-line “auction” offering sale of computer products that were never delivered. The defendant pleaded guilty to wire fraud and was sentenced to six months home detention, three years probation and ordered to pay restitution of over $22,000. He was also barred for life from conducting internet commerce.

In United States v. Middleton,85 the court held that the term “individual” as used in the Computer Fraud and Abuse Act, is not confined to natural persons, but extends to business entities, and hence damage to an ISP-victim was encompassed under the statute.

In United States v. Hoke,86 a suit was filed against Gray Hoke for disseminating misinformation on a counterfeit Bloomberg News Service Web page regarding an alleged merger between his employer PairGain

83 The London Metropolitan Police website maintains an excellent section on 419 Advance Fee Fund (AFF) Fraud.
84 S.D. Fla. 4/*/98 (USA)
85 35 F. Supp. 2d 1189 (N.D. Cal. 1999) (USA)
86 Magistrate No. 99-889M (C.D. Cal. 4/14/99) (USA)
Technology, Inc. and ECI Telecom Ltd. Initial investigation by the FBI revealed that Hoke might use services of Angelfire.com to host the page and Hotmail email service. Hoke was traced by IP addresses from these services. Hoke pled guilty and was sentenced to five months of home detention, five years probation, and restitution of $93,086.77.

In *U.S. v. Pirello*, the defendant was found fraudulently setting computers online. He had placed four advertisements on Internet classified ads websites, soliciting buyers for computers. Pirello received three orders, deposited the money in his personal bank account, and never delivered computers. The court held defendant liable for fraud by using the Internet website to solicit orders for non-existent computers.

The *Sony.Sambandh.com Case* (2002) was the first cyber-related fraud case in which the accused was convicted. This case has sent out a message that the provisions of the Indian Penal Code can be effectively applied to certain categories of cybercrimes which are not covered under the Information Technology Act, 2000. The complainant, Sony India Private Ltd. was running a website called www.sony.sambandh.com enabled non-resident Indians to send Sony products to their relatives and friends in India after they make online payment for the products.

In May, 2002, someone logged on to the website under the identity of Ms. Barbara Campa and ordered a Sony coloured TV set and a cordless headphone. She gave her credit card number for payment and requested the product to be delivered to Arif Azim in Noida. The payment was cleared by the complainant Sony India Ltd. Who delivered the items to Arif Azim after following the relevant procedure of due

87 255 F. 3d 728 (9th Cir. 2001) U.S.A.
diligence. It also took a digital photography showing the delivery being accepted by Arif Azim.

Nearly one and a half month after this transaction, the credit card agency informed Sony (India) company that it was an unauthorised fraudulent transaction as the real owner had denied having made the purchase. Thereupon, the company lodged a complaint for online cheating to the CBI which registered a case against Arif Azim under Section 418, 419, 420 of the Indian Penal Code.

The investigation of the case revealed that the accused Arif Azim who was working at a call center at Noida gained access to the credit card number of an American national, which he had misused on the company’s website. The CBI recovered the coloured TV and cordless headphone from Arif Azim. The Court on the basis of evidence of witnesses and material before it found Arif Azim guilty of offence under Section 418, 419, 420, IPC and convicted him for cyber fraud and cheating. However, in view of the young age of the accused i.e. 24 years and this being his first conviction, the Court ordered his release on probation for a period of one year.

In Pune Citibank Mphasis Call Center Fraud, some ex-employees of BPO arm of Mphasis Ltd MsourcE, defrauded US Customers of Citi Bank to the tune of RS 1.5 crores has raised concerns of many kinds including the role of "Data Protection". The crime was obviously committed using "Unauthorised Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes". ITA-2000 is versatile enough to accommodate the

aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". Cheating", "Conspiracy", "Breach of Trust" etc are therefore applicable in the above case in addition to section in ITA-2000. Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damage to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

In yet another case, i.e. Infinity e-search (Gurgaon BPO), a young person Karan Bahari aged 24 years was working for a Gurgaon based website designing and online marketing firm Infinity e-search. He was alleged to have fraudulently sold information on 1000 bank accounts of British customers from an Indian call centre to an undercover British journalist working for a British newspaper, ‘The Sun’ for 2750 pounds. The employee karan, however, denied the charge and claimed that he was only a middleman and that he did not sell data collected by his employer i.e. Infinity e-search company. The company also denied any involvement in the case as it did not handle any data for the bank named in the said newspaper and that his employee Karan Bahari did not have access to confidential data of any kind.

In this case, it was alleged that the British journalist for “The Sun” used Karan Bahari who was working in the Infinity e-search, as an intermediately, offered him a job and requested for a presentation on a CD and later claimed that the CD contained confidential data about thousand bank accounts of British customers who were customers from an Indian call centre. However, on investigation, the fact that the CD

90 Decided by Delhi High Court on June 24, 2005.
contained such data could not be substantiated by the journalist and therefore, the charges of fraud could not be proved against Karan Bahari or his employer i.e. the infinity e-search company. But the case has raised on apprehension that there is possibility of an anti out-sourcing backlash if Indian online companies do not take sufficient care of the data which they handle.

The Supreme Court’s ruling in the Morgan Stanley’s case\(^9\) has been instrumental in augmenting Business processing Outsourcing (BPO) with a view to creating a global safe-deposit vault to halt data theft and improve India’s prospects as an outsourcing destination. The National Association of Software and Services Companies (NASSCOM) announced setting up an independent watchdog self regulatory organization (SRO) in April, 2007 for setting out data security standards for the software industry with focus on global practices.

**d. Judicial Response on Credit Card Fraud:**

Credit card fraud is a wide ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorised funds from an account.

The credit card frauds have assumed dangerous proportion throughout the globe. In USA, the ten most frequent fraud reports involve undelivered services, damaged, defective, misrepresented or undelivered merchandise, auction sales, pyramid schemes and bogus marketing of goods and of the most predominant among them is credit card fraud. It is estimated that half of a billion dollars are lost by the consumers through credit card frauds.

In Delhi Credit Card Fraud Case,\textsuperscript{92} Court of Metropolitan Magistrate Delhi found guilty a 24 year old engineer working in a call centre, of fraudulently gaining the details of Campa’s credit card and bought a television and a cordless phone from Sony website. Metropolitan Magistrate Gulshan Kumar convicted Azim for cheating under sections 418, 419, 420 of the IPC, but did not send him to jail. Instead, Azim was asked to furnish a personal bond of Rs. 20,000 and was released on a year’s probation.

In Hotel Le Meridien, Pune Case,\textsuperscript{93} almost 30 customers of Hotel Le Meridien, Pune were cheated. Four persons were creating duplicate credit cards from those belonging to customers and then using them to make purchases. One of the person was a cashier at the Chingari Restaurant in Hotel Le Meridien, and he used credit card skimmers and readers which recorded details of the credit card being swiped. These details were then copied on blank cards with magnetic strips. Altogether they used 33 cards of 27 banks among themselves to go on a shopping spree, with the total amount of such purchases being pegged at Rs. 1 crore. The type of cards being targeted were the higher end ones, namely, Gold, Titanium, Platinum and corporate cards, where the credit limit was higher. This came to light when a Citibank employee went to the hotel with some friends and lodged a police complaint after getting his card bill with exorbitant purchases that he had no idea about.

e. Judicial Response on Defamation:

Every person has a right to have his reputation preserved inviolate. This right of reputation is acknowledged as an inherent personal right or every

\textsuperscript{93} Ibid.
person. It is a *jus in rem*, a right good against the entire world. A man’s reputation is his property, more valuable than other property.\(^9^4\)

According to Wikipedia, Cyber Defamation is a crime conducted in cyberspace, usually through the Internet, with the intention of defaming others. Sending defamatory email, writing derogatory comments on facebook, orkut or other social networking sites also constitutes cyber defamation. The Internet can be used to spread misinformation, just as easily as information. Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators. Minors are increasingly using web forums and social networking sites where such information can be posted as well. Criminal behavior can include the publication of intimate photographs or false information about sexual behaviours.

In the American case of *Cubby Inc. v. CompuServe Inc.*\(^9^5\) action was brought by the plaintiff company against the defendant company CompuServe for its alleged publication of defamatory libel and unfair business tactics through computer network. The District Court held that, “the computer service that provides subscribers with access to electronic news or publication put together by independent third party and loaded into company’s computer website was a mere ‘distribution’ of information for which it could not be held liable for defamatory statements made in the said news or publications unless it is shown that computer company knew or had reason to believe of the existence of such defamatory contents”. The court further ruled that just as a public library, bookstore or news stand does not have any editorial control over

---

\(^9^4\) Dixon v. Holden, (1869) LR 7 Eq 488.
\(^9^5\) (1991) 776 F. Supp. 135 (USA)
the publications it distributes so also a computer company does not have any control over the publications it distributes so also a computer company does not have any control over its publications nor is it feasible for it to examine the contents of any publication and see if it carries any defamatory statements.

The High Court noted that computer technology is rapidly transforming the information industry and a computerized database is the functional equivalent of a traditional news vendor or distributor. Therefore, it cannot be held liable for defamatory contents of the publication unless it is shown that it had the knowledge or knowledge or reason to believe about the existence of such libellous contents thereof.

The decision in the Cubby’s case96 was reaffirmed by the Supreme Court of New York in Stratton Oakmont v. Prodigy,97 and it was reiterated that Computer Bulletin Boards are just like books stores or libraries. But in the instant case, the defendant Prodigy had his own policies and technologies relating to posting on the bulletin boards which charged the character of his computer services from distributor to that of a publisher and therefore, it had to accept liability for legal consequences flowing out of the defamatory statements made against the plaintiff.

In Firth v. State of New York,98 the plaintiff claimed that publication of an alleged libel on the internet was “continuous publication”, which would extend the statute of limitation. The court held that the statutes would run from the date the material was first posted, rather than continuously. On October 29, 2001, the New York Appellate Division Court affirmed the decision.

96 Ibid.
98 N.Y. Court of Claims, March 2000 (USA)
In *Norway v. Tvedt*,\(^9^9\) the accused was the founder of a far right group in Norway. He was convicted for posting racist material that mixed neo-Nazism, racial hatred, and religion, on a website. He was held responsible for the material despite the fact that it was posted on a server that was based in the United States.

The Indian Penal Code, 1860 also highlights that defamatory statement need to be published (or communicated). The Supreme Court held in *Bennett Coleman & Co. v. Union of India*\(^1^0^0\) that “publication means dissemination and circulation”. That is, communicating defamatory statements only to the person defamed is not publication.

The landmark case of *S.M.C. Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra*\(^1^0^1\) was the first case of cyber defamation in India, the High Court of Delhi assumed jurisdiction and passed an order of ex-parte injunction against the defendant restraining him from damaging the reputation of the corporate entity, of which he was an ex-employee. The accused Jogesh Kwatra was sending derogatory, defamatory, obscene, vulgar, filthy and abusive e-mails to his employers and Managing Director Mr. R.K. Malhotra in order to malign the high reputation of the company and its subsidiaries all over India and abroad. The plaintiffs contended that such defamatory e-mails by the defendant were in blatant violation of their legal right and the motive of the defendant in sending such defamatory e-mails was to retaliate against the termination of his services of by the management of the company. On the basis of evidence produced before the Court, the defendant was found guilty of cyber defamation therefore; the High Court of Delhi passed an ex-parte ad

\(^9^9\) Asker and Baerum District Court (Norway, 2002) (NORWAY)
\(^1^0^0\) (1972) 2 SCC 788.
\(^1^0^1\) Petition No. 1276/2001 decided by the Delhi High Court in 2003.
interim injunction against the defendant restraining him from sending the said defamatory, obscene, vulgar and abusive messages.

In Gremach Infrastructure Equipment and Projects Limited and Others v. Google India Private Limited, Google Inc. is the owner of the popular blogging platform Blogpost. Blogpost hosted a blog by one toxicwriter (a pseudonym chosen by the blogger to mask his/her identity). The writer had allegedly written certain defamatory comments about an Indian Mining Company. The Bombay High Court found the posting prima facie defamatory and ordered Google to reveal toxicwriter’s identity. This is only the interim order. It is unclear as to whether the company has asked for damages against Google (and whether safe harbors will come into play).

Google sought to comply with the order as not only the blog which was available at www.toxicwriter.blogspot.com but also its cache is available on Google. A few snapshots though were made available on another website. Free Speech and Privacy issue notwithstanding Google may give the identifying information of the blogger. The reason for this is its own privacy policy. It stated that, “[w]e have a good faith belief that access, use, prevention or disclosure of such information is reasonably necessary to satisfy any applicable law, regulation, legal process or enforceable governmental request.

In Tata Sons v. Greenpeace International, Justice S. Ravindra Bhat, authoring the judgment noted that, though the internet has a wider reach and potential for injury, traditional standards for the grant of injunctions in cases of libel will be applicable. The court reasoned that these traditional standards are well developed and there is no

---

102 508/2008 Bombay HC, Order passed by Justice D.Y. Chandrachud.
constitutional mandate which allows the court to create a differentiation. If this reasoning is strictly applied it would mean that the conventional rules of defamation. If applied liberally, courts may in cases of a legislative vacuum, apply other developed legal principles without differentiation. [Cyber defamation Injunction not granted].

In the case of Tata Sons vs. Turtle International, the Delhi High Court has held that publication is a comprehensive term, embracing all forms and mediums â€“ including the Internet. That an internet publication has wider viewership, or a degree of permanence, and greater accessibility, than other fixed (as opposed to intangible) mediums of expression does not alter the essential part, i.e. that it is a forum or medium. There is much sense to have more defined criteria taking into account the nature of the internet content. Injunctions on internet content should not be readily granted (especially ex-parte) since, firstly the internet is an easy, self publishing platform providing a medium of expression for marginal individuals not having corporatist outlets. Secondly, the internet facilitates the distribution of content for a minor cost to a vast audience. Both the alleged injury and the free speech concern are greater due to the wider dissemination of the content. These are only some of the concerns which set the internet apart and it is desirable to have a nuanced appreciation.

f. Judicial Response in Protection of Intellectual Property Rights:

The judiciary has always responded to the need of the changing scenario in regard to development of technologies. It has used its own interpretative principles to strike a balance between the age-old rigid laws and the advanced technological knowledge. Internet and other
information technologies have brought with them certain issues which were not foreseen by the legal regime earlier. Various new developments leading to different kinds of cybercrime unforeseen by the Parliament have come to fore in the new millennium. As regards the internet related IPR disputes arising as a result of development of computer science, the courts have played a role of an umpire between the contesting litigants so as to ensure that no injustice is caused to anyone.

The concept of intellectual property comprises a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights, is an offence punishable under Section 43 of the Information Technology Act, 2000. Software piracy is a common form of IPR violation. Some other IPR violations include copyright infringement, trademark and service mark violation, theft of computer source code etc. The relevant case law indicating judicial trend in regard to online IPR violations and offences are briefly discussed in the succeeding paragraphs.

In Himalaya Drug Co. v. Sumit,\(^{104}\) the plaintiffs were engaged in the manufacture and sale of Ayurvedic medicinal preparations and had developed a website under the domain name www.himalayadrugco.com. They had spent considerable time, labour, skill and money in preparing database of more than 209 herbs. It came to the notice of the plaintiffs that the defendants were operating a website which reproduced the plaintiffs entire herbal database by copying the preliminary information of each herb and the detailed monograph, so much so that even the synthetically and grammatical form that appeared on the appellant’s website was copied verbatim by the defendant in their website.

\(^{104}\) 2006 (32) PTC 112 (Del).
The appellants, therefore, moved the Delhi High Court for an injunction alleging that the defendants were passing off their business using the similar domain name as that of the appellant’s which was causing deception and confusion among the consumers and the public. The defendants having failed to respond and attend the Court despite several notices, the High Court of Delhi proceeded ex-parte against the defendants and ordered a permanent injunction restraining them from reproducing, using and/or communicating to public on their herbal website which they had copied from the appellant’s database. The Court also awarded punitive damages to the extent of eight lakhs rupees, which the defendants were required to pay to the plaintiff by way of compensation.

i. Judicial Response in Protection of Trademark:

In the case of Kirloskar Disel Reconstruction (P) Ltd. v. Kirloskar Proprietary Ltd.,\(^{105}\) the High Court of Bombay held that the definition of trademark includes within it the word ‘mark’, which mean name and therefore, the term ‘trademark’ in Section 105 (c) of the Trademarks Act must be considered to a comprehensive term including within it the ‘trade name’, or the ‘business name’ and the name by which the article or goods are sold. Obviously, there should be a reasonable nexus between the mark used in relation to the goods and the person claiming right to the use of that mark. In this case, the Court restrained the defendant from using the trade name ‘Kirloskar’ for their proprietary companies as there was likelihood of confusion or deception of the public resulting in damage to the plaintiff. In other words, a passing off action would lies in cases of trademark or trade name violation. The defendant was therefore,

---

105 AIR 1996 Bombay. 149.
restrained from using the name ‘Kirloskar’ in their online advertisements and internet communications.

In Banyan Tree Holding (P) ltd. v. A. Murlikrishna Reddy, the High Court of Delhi held that in a commercial transaction entered into by the defendant with internet users located within the jurisdiction of the forum Court, there is no possibility of solitary trap-transaction because it will not be a case of purposeful availing.

In the instant case, the plaintiff was operating his business from Singapore whereas the defendant was using Banyan Tree holding trademark in dealing with customers on internet. In a passing off action against the defendant the Single Judge deferred the matter to the Division Bench on ground that plaintiff and defendant both were not within the jurisdiction of the present Court. It was contented on the behalf of the plaintiff that the Court has the jurisdiction for passing off action universally where the matter relates to dealing on internet and the defendant had purposefully availed himself of the jurisdiction of the forum Court to defeat plaintiff’s claim. The Division Bench allowed the appeal and held that it had the jurisdiction because the internet user was located within its jurisdiction. The defendant was therefore, restrained from using the plaintiff’s trade name on internet.

In the case of TATA & Sons v. A.K. Choudhri, the petitioners used TATA logo in its website for its products. They sued the defendant for openly selling his steel and cutlery and similar items using deceptively similar trademark on the website, and prayed the Court for an injunction directing the respondent to refrain from selling their products using brand name similar to that of the petitioners. Allowing the petition,
the High Court of Delhi ruled that petitioner’s trademark had acquired unique goodwill and reputation and it had become a distinctive trademark within the meaning of Section 9 of the Trademarks Act due to its long continuity. Therefore, the court prohibited the defendant from using the trademark under Section 29 (4) of the Act although it was not being used by the respondent for commercial purposes.

ii. Judicial Response on Software Piracy

Software piracy is unauthorised copying and use of Software without proper license, simultaneous use of single user license software by multiple users or loading of single user license software at multiple sites, also amounts to software piracy. It is not possible to completely eliminate Software piracy, but the same can be controlled by enforcing the laws and generating awareness in the society. Under the IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008, According to Section 66, any accused who has committed software piracy shall be liable to pay damages by way of compensation to the person so affected also the affected person can file a Criminal Complaint under Section 66-B of Copyright Act, 1957 and under Section 120B, 420, 468 & 471 of the Indian Penal Code, 1860 in the nearest Police Station where the above crime has been committed.

Whelam Association Inc, v. Jaslow Dental Laboratory Ltd.108, is considered as a landmark judgment on software piracy. Answering in the affirmative, the Court held that the non-literal elements of a computer program are not copyrightable because the purpose of the program would be idea and everything else would be a part of expression, which is copyrightable. In this case, the court held that it is not necessary for the

108 (3rd. Cir. 1986) 797 F2d 1222 (US).
computer’s program’s purpose or function including its structure, sequences and organization.

In Autodesk, Inc. and Another v. Mr. Prashant Deshmukh and Others, the court raised concerns about increasing instances of privacy of software of reputed companies such as Microsoft and AutoCAD in the country, which might cause discouragement amongst the investors in the development of such software in the lack of dwindling license fees. Furthermore, the use of pirated software for commercial rather than personal purposes should, according to the court, be more heavily frowned upon, and therefore the court awarded the plaintiffs the permanent injunction sought for as also punitive damage amounting to Rs. 1 lakh against defendant.

iii. Judicial Response on Copyright Violation:

Copyright infringement (or copyright violation) is the unauthorised or prohibited use of works covered by copyright law, in a way that violates one of the copyright owner’s exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works.

In Lotus Development Corporation v. Pareerback Software International, it was held that commuter programs like any other works are copyrightable.

A & M Records, Inc. v. Napster, Inc. was a landmark intellectual property case in which the United States Court of Appeals for the Ninth Circuit affirmed the ruling of the United States District Court

for the Northern District of California, holding that defendant, peer-to-peer (P2P) file-sharing service Napster, could be held liable for contributory infringement and vicarious infringement of the plaintiffs’ copyrights. This was the first major case to address the application of copyright laws to peer-to-peer file-sharing.

**Taj Television v. Rajan Mandal & Others**\(^{112}\) is a landmark case on copyright violation. The Delhi High Court granted a path-breaking order authorizing a court appointing a commissioner to enter the premises of any cable operator in India and record evidence of any unauthorised telecast of the FIFA World Cup football matches.

In the present case, the Plaintiff, Taj Television Ltd., based in Dubai, owned and operated an exclusive sports channel by the name of TEN SPORTS. The Plaintiff had acquired the exclusive rights to the telecast of the FIFA World Cup Football matches for India and certain other South Asian countries, from Kirch Sports, an entity that had in-turn acquired the worldwide rights from FIFA. Ten Sports was being broadcasted from Dubai in an encrypted form and could be received by only those cable operators with a decoder.

In **Dalgit Titus, Advocate and others v. Alfred A. Adevare and others**\(^{113}\) decided by the Delhi high Court, the plaintiffs were running a law firm which consisted of advocates specialized in different fields. The defendants were working with the plaintiff’s firm and were paid remuneration while they retained control over the professional organization. They claimed copyright over the work which they had done while working in the plaintiff’s legal firm. The plaintiff’s, on the other hand, contended that since the defendant’s were a part and parcel of the

---

112 FSR 22, 2003 Delhi High Court.
113 2006 (32) PTC 112 (Del).
plaintiff’s firm, they could not claim exclusive right in respect of database of the list of clients and the expert opinions and advice rendered to them as they were under an obligation to maintain confidentiality. The plaintiff also claimed to have spent substantial amount of money, time, skill, computer network, law library, office infra-structure etc.

Consequent to this dispute which arose regarding the copyright ownership between the plaintiff’s and the defendants, the plaintiffs filed a complaint before the Court that one of the defendants came to their office after the office hours and downloaded 7.2 GB of database of their crucial data, write-up through plaintiffs local area network and allegedly have stolen the hard copies compressed over ten proprietary drafts of the plaintiffs and therefore, they prayed for protection of their exclusive data under the Indian Copyright Act, 1957.

After hearing both the parties, the Court came a conclusion that plaintiff had prima facie in the database which the defendants had taken away from the plaintiff’s office. The Court noted that the defendants were free to carry on their legal profession, utilizes the skill and information they had mentally acquired by experience gained from working with the plaintiff’s legal firm but restrained them from copying material of the plaintiff in which the plaintiffs alone had the exclusive copyright. The principle of law laid down in the case clearly envisages the need for a careful drafting of different clauses of the contracts before entering into any kind of relationship, particularly the clause dealing with database and in case of a legal firm, whenever an employee of a solicitor firm drafts a document, the employer is the first owner of the copyright document.¹¹⁴

¹¹⁴ Narayanan on copyright and Industrial Design (3rd ed.) para 6 and 28.
In *Hindustan Times v. www.legalpundits.com*, a recent decision that has ramifications on free distribution of online content, the Delhi High Court passed an ex-parte interim injunction against the website for carrying and forwarding articles published by Hindustan Times (HT) Media group. The Website www.legalpundits.com, was allegedly found to have been picking new items from HT’s online portals. Further, the website was found to be forwarding the content to the public without any consent, authorization or license of the content owner, HT media group, and that too for final considerations.

HT media group had moved to the court against the websites on grounds of copyright infringement, trademark violation and unfair trade practice. HT Media also claimed damages of INR 20 lakh from Legalpundits, in the complaint.

The case *Microsoft Corporation v. Yogesh Papat, Delhi High Court*. Concerns the infringement of copyright in software and notably the interpretation of section 51 and 55 of the Copyright Act, 1957. The Microsoft Corporation, the registered proprietor of the trademark MICROSOFT, requested a permanent injunction restraining the defendant, its directors and agents from copying, selling, offering for sale, distributing or issuing to the public counterfeit or unlicensed version of Microsoft’s software program in any manner that amounts to infringement of Microsoft’s copyright in the computer programs, related manuals and Microsoft’s registered trademarks. Microsoft also requested that the defendant be prevented from selling and disturbing any product to which the trademark MICROSOFT or any variants of this trademark have been applied.

---

116 Ibid. P-273.
The defendant did not appear before the court, so the proceedings took place ex parte. The court eventually ruled against the defendant, who was downloading Microsoft software onto the hard drives of computers that if then sold, without a licence or permission to do so from Microsoft.

The court approached each piece of evidence in turn and, based on the assumption that 100 computers were sold each year and on the evidence of the software’s popularity, held that Microsoft had suffered a total profit loss of Rs 1.98 million, plus interest at 9% from the date of the decree of until the date of payment.

The court, quoting an observation by Justice Laddie in the High Court of England and Wales in *Microsoft Corporation v. Electrowide Ltd*,117 held that the defendant’s action “constituted a general threat to infringe the copyright in the class of software”. Justice Pradeep Nandrajog, who presided in the case, stated that:

“It stands established that the defendant has infringed the plaintiff’s copyright by making illicit copies of the operating systems software by openly systems software openly copying whatever operating system is currently saleable.”

**g. Judicial Response on Cyber Squatting:**

USA has passed an Act known as Anti-Cyber Squatting Consumer Protection Act 1999 to deal with this problem. Cyber squatting according to the United States federal law known as the Anti-cyber squatting protection act, is registering, trafficking in, or using a domain name with bad faith internet to profit from the goodwill of a trademark

---

117 Ibid.
belonging to someone else. The cyber squatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price.\(^{118}\)

In *Playboy Enterprises Inc v. Asia Focus International*,\(^ {119}\) defendant Asia Focus international maintained website using the domain names asian-playmates.com and playmates-asian.com in connection with pictures of adult nude women and related merchandise. Determining that the playboy mark deserves a high degree of protection as a strong mark, the court that decided that the use of the two domain names infringed on playboy’s ‘playmate’ trademark. The court emphasized the similarity of the goods and service offered and indicated that the difference between the registered mark ‘playmate’ and the domain names were minimal. In determining the use of the domain name also diluted the ‘playmate’ mark, the court focused on the intent of the defendant.

In *Panavision v. Toeppen*,\(^ {120}\) Dennis Toeppen had registered a multitude of domain names incorporating famous trademarks including Panavision.com. When contacted by Panavision, owner of the trademark, he offered to sell the domain name to them for USD 13,000. Toeppen had previously offered similar sales to other trademark owners for domain names incorporating their marks (Intermatic and American Standard). Panavision filed suit claiming trademark dilution. Toeppen argued that the requirements for dilution were not met because his use of the domain name to display the city of Pana, it did not constitute commercial use. The court determined that Toeppen’s business is to register trademarks as domain names and then sell them to the rightful trademark owners. As

---


\(^{119}\) 1998 WL 724000 (EDVa) USA

\(^{120}\) 141 F 3d 1316 (9th Cir 4/17/98) USA
such, they found the requisite commercial use. Panavision establishes the principle in cyber squatting cases that an offer to sell a domain name to the trademark holder constitutes use in commerce purpose of trademark infringement. Establishing commercial use, however, is not sufficient. The plaintiff must also show that there has been dilution. Here the ninth Circuit indicates that a court need not rely on the traditional definitions of blurring or tarnishment to find dilution. Because Toeppen’s conduct diminished the capacity of the Panavision marks to identify and distinguish Panavision’s goods and services on the Internet, the court finds that dilution has occurred. While this is one of the older case and its interpretations have been questioned by scholars, it has frequently been relied on by courts throughout the US in subsequent cases.

**Yahoo Inc. v. Aakash Arora**,121 was the first case in India with regard to cybersquatting, where the defendant launched a website nearly identical to the plaintiff’s renowned website and also provided similar services. Here the court ruled in favour of trademark rights of U.S. based Yahoo. Inc (the Plaintiff) and against the defendant, that had registered itself as YahooIndia.com. The court observed, “it was an effort to trade on the fame of yahoo’s trademark. A domain name registrant does not obtain any legal right to use that particular domain name simply because he has registered the domain name, he could still be liable for trademark infringement”.

The Bombay High Court in **Rediff Communication v. Cyberbooth & Another**122 observed that the value and importance of a domain name is like a corporate asset of a company. In this case the
The defendant had registered a domain name radiff.com which was similar to rediff.com. The court gave a decision in favour of the plaintiff.

In *Bennett Coleman & Co Ltd. v. Steven S Lalwani* and *Benett Coleman & co Ltd. v. Long Distance Telephone Company*, the arbitration panel gave a decision in favour of the plaintiff. In this case the respondent had registered domain names www.theeconomictimes.com and the www.timesofindia.com with network solutions of the United States. These two names are similar to the names of the Plaintiff’s websites www.theeconomictimes.com and the www.timesofindia.com. Another important fact was that the respondent’s websites using the domain names in contention redirect the users to a different website www.indiaheadlines.com which provided India related news.

In *Mahindra and Mahindra Ltd. v. Ajay Kumar*, the M&M company lodged complaint against the cyber squatter Ajay Kumar that the latter was using former’s domain name ‘mahindra.com’ and has transferred his original address in India to one in the United States in order to escape the jurisdiction of the Indian Courts. Disposing of the complaint, the WIPO arbitration centre (World Intellectual Property Organisation’s arbitration centre) upheld the claim of M&M. Earlier also M&M had to move the WIPO centre for taking back their domain names mahindra.net and mahindre.org from the same respondent (Ajay Kumar) in which they had succeeded. The contention of Mahindra & Mahindra in this case was the trademark ‘Mahindra had been registered both in India as well as in United States. The WIPO’s penalists decided in favour of Mahindra & Mahindra and held that ‘mahindre.com’ was identical to the trademark ‘Mahindra’ to which the respondent had no right.

123 Cases no. D2000-0014 and 2000-0015, WIPO.
In *Satyam Infoway Ltd. v. Sifynet Solutions*,\(^{125}\) the Respondent had registered domain names www.sifynet.com and www.siffynet.com. Satyam (Plaintiff) had an image in the market and had registered the name Sifynet and various other name with ICANN and WIPO. The word Sify was first coined by the plaintiff using elements from its corporate name Satyam Infoway and had a very wide reputation and goodwill in the market. The Supreme Court held that “domain names are business identifiers, serving to identify and distinguish the business itself or its goods and services and to specify its corresponding online location”. The court also observes that domain name has all the characteristics of a trademark and an action of Passing off can be found where domain names are involved. The decision was in the favour of the plaintiff.

**h. Judicial Response on Phishing:**

According to Wikipedia phishing means, in the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as username, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is the fraudulent acquisition, through deception, of sensitive personal information such as passwords and credit cards details, by masquerading as someone trustworthy with a real need for such information. It is a form of social engineering.

Under the IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008 Section 66-D is applicable and Section 379 & 420 of Indian Penal Code, 1860 are also applicable.

---

\(^{125}\) 2004 (6) SCC 145,
In **State v. Johnson Nwanonyi and Michel Obiorahmuozboa, Anambra State in Nigeria**, a local court in Malappuram district in Kerala sentenced two Nigerians to five years rigorous imprisonment on July 20, 2011 in a cyber crime case. The two had cheated a doctor in the district of Rs. 30 lakh about two years ago. Johnson Nwanonyi (32) and Michel Obiorahmuozboa (34), both hailing from Anambra state in Nigeria, were sentenced each other section 420 (cheating)- 5 years, and 468 (forgery)- 5 years of IPC and section 66D (phishing) of Information Technology (Amendment) Act, 2008-2 years and a fine of Rs. 1.25 lakh by a Chief judicial Magistrate V Dileep in Manjeri in Malappuram district. The sentence would run concurrently.

According to the charges filed by the Karipur police, the duo had cheated the doctor Dr. C. Chomas, hailing from Valluvambram in Malappuram district after they sent an e-mail inviting application to recover a huge sum of unclaimed money left behind by a Nigerian businessman. They had advertised that the money, kept aside for charitable hospital, was lying unclaimed in a bank. When the doctor responded to the e-mail, they tricked him by asking to pay Rs. 30 lakh as processing fee. But a planned move by the police and the doctor succeeded when the Nigerians were lured into Kerala in March 2010. They were then arrested by the Karipur police. The strong evidence based on which the prosecution presented the case became crucial in the first verdict against financial fraud under the IT Act.

The case of **National Association of Software and Service Companies v. Ajay Sood and others**, ruled that phishing on the

---

127. The Judgment in the case was delivered by the Delhi High Court on March 12, 2005.
internet is an illegal act entitling the victim for an injunction and recovery of damages just as in case of passing off.

In the instant case, the plaintiff i.e. National Association of Software and Service Companies having its trade name NASSCOM, was the India’s premier software association and the defendants were running an employment agency providing employment and recruitment opportunities to job-seekers. In order to obtain personal data, which they could use for the purposes of recruitment, the defendants composed and sent e-mails to the concerned parties in the name of NASSCOM. On a complaint from the plaintiff, the High Court of Delhi passed an ex-parte ad interim injunction restraining the defendants from using the trade name or any other name deceptively similar to NASSCOM. The Court further restrained the defendants from representing themselves as being associated as a part of NASSCOM and ordered a search of the defendant’s premises by a local Commission.

On the basis of two hard disks of computers recovered from the defendants it was found that the e-mails were sent by the defendants to fictitious persons in order to hide their illegal fraudulent activities. The investigation also revealed that the defendants had collected huge amount of money by fraudulently using the NASSCOM’S trade name. Finding no other way to escape liability and punishment, the defendants admitted their crime and the parties agreed to a mutual compromise under which the defendants were to pay 1.6 million rupees to the plaintiff’s by way of damages for violation of plaintiff’s trade name rights. The hard disks seized from the defendant’s possession were ordered to be handed over to the plaintiffs who would be the sole owner of those disks.
This case is considered as a landmark decision in the history of Indian cybercrimes for two obvious reasons. Firstly, phishing is punishable as a cyber offence although there is no specific statutory legislation to this effect; and secondly, it reaffirms the faith of intellectual property owners that their intangible property rights are well protected by the judiciary.

The Court in this case expressed a view that of late, phishing has developed as a sophisticated method of committing organized cybercrime by befuddling even the most experienced and knowledgeable persons. Phishing criminals sneak into a computer network or a social networking site and obtain e-mail addresses of the people and create messages that purport to come from direct bosses. They manipulate legitimate websites to redirect e-mails to bogus sites that collect victim’s information.

In Mount Everest Mineral Water ltd. v. Bisleri International Pvt. Ltd. and others, the petitioner held registration for trademark “Himalayan” in respect of mineral water since 2002. He filed a suit against respondent Bisleri International (P) Ltd. seeking to restrain him from using the trademark ‘Himalayan’ which was allegedly deceptively similar to petitioner’s trademark. The respondent challenged the validity of registration of two trademarks except the one which considered of the word “HIMALAYAN” per se in respect of “Mineral Water” holding the said registrations were not justifiable. Therefore, the entries in the register in respect of those two trademarks should be considered to have been wrongfully made in the register. Rejecting the contentions of the respondents, the Court allowed the petition on the ground that a trademark cannot be declared invalid if it has acquired distinctiveness after the grant of a registration and before the challenge to the validity of

such registration. Also, the written statement filed by respondent makes no reference to Section 26 of the Geographical Indication of Goods (Registration & Protection) Act, 1999, which protect marks registered prior to 15th September, 2003, the date when the said legislation was notified and came into force. The writ petition was therefore, allowed with cost of Rs. 10,000/- to be paid by respondent (BIPL) to the petitioner within four weeks from the date of judgment.

i. Judicial Response on Online Gambling:

Gambling in India is prohibited under the Public Gambling Act 1867. However the word ‘gambling’ is not defined in the Public Gambling Act 1867. According to the Supreme Court of India, “Gaming is the act or practice of gambling on a game of chance. It is staking on chance where chance is the controlling factor. Internet gambling is traditional crime of gambling where computer is used as tool provided it is otherwise is an offence in a particular jurisdiction.129

There are thousands of Websites that offer online Gambling. The special issue with online gambling is that it is legalised in several countries. So legally the owners of these websites are safe in their home countries. Virtual casinos, Cases of money laundering etc are online cases.130

The law related to gambling is also applicable to online gambling. All gambling contracts are considered to the wagering contracts and it is not possible to enforce such contracts under the ICA, detailed above.

In Minnesota v. Granite Gate Resorts, Inc., the policy Minnesota’s attorney General had stated in its Internet warning was tested in court. The Attorney General had asserted the right to regulate the activities of 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. The court defined the defendant’s motion to dismiss for lack of jurisdiction because of hits from Minnesota at the defendant’s Website, the availability of a toll-free number that users could call advertised on its Web page, and the number of Minnesota resident who had signed on to the defendant’s mailing list.

Relying on inset, the court held that defendant’s advertising on the Internet constituted a direct marketing campaign directed at residents of the state of Minnesota, which was sufficiently purposeful to subject the defendant’s to suit in the forum state.

In Olivier v. Ministry of Safety and Security, Province of Gauteng, on application of owner for return of certain computer equipment seized in a search, a South African court held the impoundment lawful on the grounds that it was used for online gambling in contravention of South African law.

In State of New York v. World Interactive Gaming Corp, Court granted injunction barring Antigua-based online gaming company from doing business with New York residents. The court held that regardless of whether gambling is legal where the company is based. “Te

132 Thomas E. Jensen, Supra note 81, at 4.
133 Kravitz, supra note 15, at 1.
134 High Court of South Africa, Witwatersrand Div., 10/97 (SOUTH AFRICA)
act of entering the bet and transmitting the information from New York via the internet is adequate to constitute gambling activity within New York State”.

The company required users to enter a physical address was in a state where gambling was illegal. However, the New York attorney general used Nevada address from New York and was able to gain access. The court held this attempt to screen users was not sufficient to shield the site from liability.

Recent Indian Cyber Lotto Case\textsuperscript{136} was very interesting on online gambling. A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a website and an email address on the Internet with the address ‘eurolottery@usa.net.’ Whenever accessed, the site would name him as the beneficiary of the 12.5 million pound. After confirmation a Telugu newspaper published this as a news. He collected huge sums from the public as well as from some banks for mobilization of the deposition in foreign currency. However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs. 1.73 million bounced. Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

j. Judicial Response on Cyberstalking:

Stalking in common parlance means a harassing or threatening behavior which an individual exhibits towards the other. If an individual uses cyberspace for stalking then it is called cyberstalking. Thus, cyberstalking is an online course of conduct of a person by which the

\textsuperscript{136}Prashant Mali: Cyber Law & Cyber Crimes, 1st Edn. 2012, Snow White Publications. P-85
targeted person is terrorized, embarrassed, ashamed, molested, outraged, or frightened.

Stalking is not a new phenomena. This offence was being perpetrated in real space also. The stalking by former friends or employees or by a man to women has been in practice with a desire to force the targeted party to come to the terms of stalker. The use of cyberspace for stalking has not only widened the reach of the stalker, as he can now reach to any part of the globe, but he can now impersonate the victim to harass or humiliate him. It is now not necessary for stalker to disclose his identity.

In People v. Alan Munn, the defendant in a harassment case, who asked the readers of a posting on an internet news group to kill a police officer with family, moved to dismissed on the grounds that New York statute did not cover the internet. Statute covered communications “by telephone, or telegraph, mail or any other form or written communication”. The judge held that posting was covered because it was initiated by means of telephonic communication with the network community.

In an Australian case R v. Vose an older male stalked a young boy, following him with a camera and placing updates of his activities on his personal websites, including descriptions of his paedophilia and of his potential dangerous to those who threatened him. The offender was charged with stalking.


{347}
Mrs. Ritu Kholi Case\textsuperscript{139} is a good example of cyberstalking. The gravity of cyberstalking came into focus in India when Delhi Police was asked by one Mrs. Ritu Kholi to file-complaint against an unknown person who was using Mrs. Kholi’s name to chat over the Internet for four consecutive days.

While chatting on the Net, the unknown person was posing as Mrs. Kholi, was given her address to anyone who would respond and was using obscene language. He would also encourage others to telephone Mrs. Kholi by giving her telephone number. Because of this mischief, Mrs. Kholi received 40 calls in three days mostly at odd hours from places like Ahmedabad, Bombay, Cochin and Kuwait which shattered personal life and mental peace of the victim.

The Police machinery swung into action. After making thorough investigation, the IP addresses were traced which led to the arrest of Manish Kathuria who pleaded guilty. The accused was arrested under Section 509 of the IPC and was afterwards released on bails (the case was registered before coming into force of the IT Act, 2000)

k. Judicial Recognition to Electronic Documents:

Consequent to passing of the Information Technology Act, 2000, electronic documents have come to be recognized at par with the written documents for the purpose of evidence in law. Similarly, the digital signatures\textsuperscript{140} affixed in accordance with the provision of Section 5 of the IT Act, 2000, will be considered equivalent to written signatures. All electronic documents either in the electronic form itself or as certified print-out thereof shall be admissible under the Indian Evidence Act,\textsuperscript{139, 140}

\textsuperscript{139} Farooq Ahmad: Cyber Law of India (Law on Internet), 3rd Edn. New era Law Publication, p-411.

\textsuperscript{140} The expression ‘Digital Signature’ has been replaced by the term ‘Electronic Signature’ by the I.T. (Amendment) Act, 2008.
1872. The recognition of electronic document as a valid evidence admissible under the law of evidence has been facilitated the prosecution of cyber criminals and establishing their guilt on the basis of such evidence.

Having referred to the legal provisions relating to the judicial recognition of the electronic record/document as a valid piece of evidence, it would be pertinent to refer to some of the judicial decisions where evidence was produced before the court in one or the other electronic form.

In the case of Crown Life Insurance Co. v. Craig,\textsuperscript{141} it was held that data from a computer database is a “document” within the meaning of the American Law of Civil Procedures and it must be produced as evidence in accessible form. The court in this case, rejected the argument that “written document” referred only to documents in hard copy (on paper) form.

In Armstrong v. Executive Office of the U.S. President,\textsuperscript{142} the Court expressed a view that government e-mail record is a record as defined by the Federal Records Act and therefore, it was not sufficient for the Government to preserve the paper print-outs of such messages but its data on computer tape should also be preserved.\textsuperscript{143}

1. Judicial Response on Hacking (Unauthorised Access):

Hacking means unauthorised access to computers. When a 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

\textsuperscript{142} 1 F. 3d. 1274 (1993) U.S. (Circuit Court’s Appeal 13.8.1993).
\textsuperscript{143} Timken Co. v. U.S. In this case the Court ordered production of computer database even though its paper print-outs had been produced previously.
means with intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, he is said to have committed an offence of hacking. The person who commits an offence of hacking is called hacker. Webster’s Dictionary defines the term ‘hacker’ as a computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance.

Unauthorised access is also a punishable offence under Section 1030 (a) (5) (A) of the cyber law of United States. The case of USA v. Robert Tappan Morris may be cited as illustration. In this case, the accused Morris was a research student of the computer Ph.D. program of the Carnell University in 1988. He had acquired sufficient expertise and experience in computer technology and programmed a ‘worm’ which was difficult to read or defect and released it into the computer networks. He devised four ways in which the worm could break into computers on the network. As a result of this, several computers at locations around USA either crashed or became “catatonic”. Morris realising the gravity of his illegal act, sent anonymous messages from Harvard over the network instructing programmers how to kill the worm and prevent re-infection, but the network route was clogged and this message did not reach the users.

The accused Morris was found guilty for an offence of unauthorised access to protected systems following a Jury trial and was sentenced to three years of probation, 400 hours of community service and a fine of 10,500 dollars. The US Court of Appeal held that although

---

144 Section 66 of the IT Act, 2000.
initial insertion of the ‘worm’ simply amounted to exceeding the authorised access but evidence showed that later on it was designated to spread to other computer for which he had no authority, express or implied.

In Regan Genard Gilmour v. D.D.P.,147 the accused was an administrative officer in the Debt Management and Relief Section of the Australian Taxation Department. He was assigned the work of scrutinising the applications received from tax payers for grant of relief and forward them for consideration alongwith the relevant data and document. After the grant of relief by the higher official, he was required to insert the data into compact computer system which was to be operated only by the Debt Management Section and thereafter the data was finally entered on the tax payer’s general file.

The accused had no authority to grant relief and his duties included to enter various codes into the computer system only in case the relief had been granted. But the accused intentionally entered data relief code stating grant of relief in 19 cases of tax payers knowing it well that such relief was not granted. However, the evidence showed that he had no personal gain or interest in taking this course and he did it solely in order to expedite the disposal of cases as there were lots of inconsistencies in determination of relief applications.

He was changed for an offence of unauthorised access to computer system under Section 76C of the Australian Crimes Act, 1914, and held guilty of the said offence as he was not authorised by his employers to insert the relevant data i.e. relief code “43” in the computer without specific permission of the employers prior to such insertion. The

147. C.W. case No. 60488/95 decided by Supreme Court of New South Wales (Australia).
Court held that an entry intentionally made without lawful excuse and known to be false, has to be treated as to have been made without lawful authority.

In Delhi Hackers’ Case,\textsuperscript{148} Delhi police arrested two hackers on 6\textsuperscript{th} February 2001.\textsuperscript{149} It was the most breaking news in India because two people were arrested by the Delhi police for allegation of hacking a website. This was probably the first case in India where accused were arrested; as said by police Commissioner Rajan Bhagat. Both the hackers were detained for allegedly blocking the website named goZnextjob.com. This website provides support and information to prospective employers and job-seekers. The accused posted a message on that website declaring that it was closed but actually it was very much open. The hackers were sent to judicial custody for 14 days as they were charged under section 406 of Indian Penal Code i.e. criminal breach of trust, and section 66 of the Information Technology Act 2000 i.e. offence of hacking. Though they were denied bail by the Metropolitan magistrate on 8\textsuperscript{th} February 2001 after they were arrested on 6\textsuperscript{th} February 2001; on 12\textsuperscript{th} February Additional Session judge of Delhi, Mr. P.K. Gauba granted bail to those two hackers who were the partners of software solutions Mr. Amit Pasani and Mr. Kapil Juneja.

In Hacker Kalpesh Sharma’s Case,\textsuperscript{150} on 26\textsuperscript{th} September 2003, a media news disclosed about hacker Kalpesh Sharma as he was put behind the bars in Ahmadabad.\textsuperscript{151} He was arrested on 24\textsuperscript{th} September by the Cyber Crime Branch of Mumbai police on a complaint filed by UTI Bank officials that the accused hacked the site of UTI, Banks i.e., www.uti.com

\textsuperscript{149} National Association of Software and Service Companies 2001, 10th January/news.  
\textsuperscript{151} \href{http://utcursch.wordpress.com/2006/12/17/my-answer-to-kalpesh-sharmas-allegations/}{See also “Cyber Criminal put behind bars”, ICE News Search, new media, 26th September 2003.}
on July 11 and send an e-mail to the bank authority with a message that “the website is weak and they should provide security”. He expressed that he can do good for security in exchange of Rs. 15 Lakh and posted his contact numbers. Police arrested him from Ahmadabad. He was charged under ss. 66 and 43(b) of the Information Technology Act 2000 and remanded to Police custody till October 6th as Maharashtra Government Counsel stated that the culprit has hacked many other websites and was capable to hack many others.

In Syed Asifuddin and Others. V. State of AP and Another’s,152 where a 32-bit Electronic Serial Number (ESN) of a handset provided by Reliance Infocomm under a special package to customers, had been manipulated by some employees of Tata Indicom in an attempt insert SIMs of Tata Indicom into those otherwise electronically locked handsets; the Court took it as the offence of tampering with computer source code under the meaning of section 65 of the Information Technology Act, 2000.

Under the scheme launched by the Reliance Infocomm, a customer had to use the handset along with the in-fitted Reliance SIM; and if he were to discontinue the scheme, he would have to pay some charges plus the price of the handset. Sensing the popularity of the scheme, it seems, the rival company Tata Indicom tried to enter in to what may be termed as an unfair competition, whereby some of its employees started contacting these ‘newly wedded’ Reliance customers to bring them to their fold, and reprogrammed their technologically locked handset so that Tata Indicom SIMs could fit in there.

---

152 2005 Cr LJ 4314: decided by AP High Court on 29 July, 2005.
Acting upon a First information Report filed by Reliance Indicom, the police raided some offices of Tata Indicom in Andhra Pradesh and arrested some officials of Tata Tele Services Limited for reprogramming the Reliance handsets, an offence under IPC as also Information Technology Act, 2000. The person so arrested approached the High Court requesting the Court to quash the FIR on the ground that their acts did not violate the said legal provisions.

The Court observed that under section 2 of the IT Act, 2000, a cell phone was a computer; and Electronic Serial number (ESN) and System Identification Code (SID) came within the definition of ‘computer source code’ under section 65 of the IT Act. It further observed that to alter the ESN, was tantamount to alter a computer source code, which was an offence under section 65 of the IT Act was committed; and declined to quash the FIR.

In High Court of Kerala in Feroz v. State of Kerala, held that the Government cannot unilaterally declare any computer system as protected other than the “Government work” as defined in Section 2 (k) of the Copyright Act. In this case, the Government of Kerala issued a notification under Section 70 of the Information Technology Act, 2000, declaring “FRIENDS” application software as protected system. The project envisaged development of a software for single window collection of bills payable to government department, local authorities

153 Electronic Serial Number (ESN) is a unique 32 bit-number programmed into the phone when it is manufactured by the instrumental manufacturer. ESN is a permanent part of the phone.
154 System identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.
155 Section 65 of the IT Act deals with Tampering with computer source document.
156 AIR 2006 Ker 279: 2007 (34) PTC 98 (Ker).
157 “FRIENDS” was a project comprising seven alphabets denoting Fast, Reliable, Instant, Efficient, Network, Disbursement, Services.
and various statutory government agencies etc. towards taxes, fees, charges for electricity, water etc.

A person could make payments against the government bills in a computer counter served through FRIENDS system. The work of developing FRIENDS software was entrusted to Feroz and it was first set up on Tiruanantpuram free of cost. Encouraged by the success of the project, the Government entered into a contract with Feroz to set up similar project in 13 districts of Kerala for a total consideration of thirteen lakh rupees so that the customer may avail the services of single window software facility. Feroz complied with the contract and set up thirteen software centers’ and was paid the settled remuneration.

However, a dispute between Feroz and the Kerala Government arose when government decided to modify the FRIENDS software to suit its further requirement and assigned this work to some other agency. Feroz (appellant) challenged the validity of Kerala Government’s notification issued under Section 70 of I.T. Act on the ground that it was in violation of his copyright under Section 17 (d) of the Copyright Act and was arbitrary in terms of Articles 19(1)(g) of the Constitution of India. The High Court concluded that there is no conflict between the provision of the Copyright Act and Section 70 of the I.T. Act and Section 70 is not unconstitutional as it is subject to the provisions of the Copyright Act.

Government cannot unilaterally declare any system as protected other than the government work. According to Section 17 (d) of the Copyright Act, the author of the work shall be the first owner of

158. ‘Government work’ as defined under Section 2 (k) of the Copyright Act means a work which is made or published by or under the direction or control of (i) the Government or any of its department, (ii) any Legislature in India, (iii) any Court, Tribunal or other judicial authority in India.
copyright and in the case of Government work, the Government shall, in absence of any contract to the contrary, be the owner of the copyright therein. Since there was no contract between Feroz and the Government of Kerala regarding owner’s copyright, the Government had the copyright as the work to be done by the modified system was a ‘Government-work’

m. Judicial Approach for Developing Cyber Forensics:

The term “computer forensic” was coined for the first time by the International Association of Computer Specialists (IACS) in Oregon (USA) in the year 1191. It is a branch of forensic science which is devised to identify local preserve of extract digital information from the computer system to produce and store evidence of the cybercrime before the law court. Dr. Clifford Stall, an astronomer and Professor in the University of Berkely has defined “computer forensic” as that branch of forensic science wherein cybercrime investigation and analysis techniques are applied to determine potential legal evidence in a computer environment. Internet related forensics broadly cover three areas, namely (i) computer forensics, (ii) cyber forensics, and (iii) software forensics.

Highlighting the need and importance of cyber forensics in the investigation of cyber offences, the U.S. Court in *Easely McCaleb and Associates Inc. v. Perry*¹⁵⁹ held that deleted files on a defendant’s computer hard disk drive are discoverable, and the plaintiff’s forensic expert must be allowed to retrieve recoverable files. In this case, the defendant at his own initiative had deposited the hard disk drive in question in the Court. The plaintiff moved for discovery of its contents.

¹⁵⁹ Case no. E-2663 (GA.Super. Court) decided on July 13, 1994 wherein the Court allowed the plaintiff’s expert to recover files from the defendant’s hard drives.
including files that had been deleted where they could be recovered. The Court granted permission and issued an order for reviewing electronically stored data by both the parties.

In **Eugene J. Strasser v. Bose Yalamanchi**, it was held that where a court deems it necessary to ensure adequate measures for protection of privileged data, it might order an on-site inspection of hardware to discover “purged” records. Similarly, Court has the power to appoint a neutral computer forensic expert to recover the deleted e-mails.

Computer crime or any other crime for that matter requires lot of evidence to make a small proof. Because of the intangible nature of large amount of data held in a computer which has multi-functional role, a considerable technical search expertise is required which only a competent forensic expert can handle properly. The intricacies involved in the investigation of computer crime drew attention of the investigating agencies and the courts in **Parliament Attack Case**, which took place in Delhi on December 13, 2001, wherein the Court held that investigation of such crimes has to be entrusted to specially trained investigating officials with the assistance of forensic experts who have thorough knowledge about the working of computers and its related techniques.

In **Firoz v. State of Kerala**, the Court, inter-alia, observed that cyber forensics greatly help the investigations of the cybercrime to prove the motive, means and opportunity for the criminal to commit the crime and means adopted by him. That is, the purpose which prompted the perpetrator to commit the crime and means adopted by him, namely,

---

160 (1996) 669 So. 2d. 1142 (Florida District Appeal Court, decided in April, 1996) the case relates to litigation between two plastic surgeons relating to data protection.
162 AIR 2006 Ker 279
why, how and when it was done. The motive may be anything from curiosity to money-making, revenge or misadventure.\textsuperscript{163}

The Courts in India also recognize the fact that computerized record keeping is rapidly becoming a normal procedure in the business and commercial world. Therefore, there is a greater need to develop adequate forensic mechanism and expertise in this field so that investigation of cybercrime is facilitated.

n. Judicial Response on Cyber Terrorism:

Cyber terrorism is one of the cyber crimes in superhighway or cyber world.\textsuperscript{164} It is a term esoteric, complex and difficult to circumscribe within the four corners of the definition, which will be universally acceptable. While the word “cyber” relates to cybernetics, which is our tool of trade, “terrorism” denotes an act of violence. The ambiguity in the definition of the term cyber terrorism brings indistinctness in action as Dorothy Denning points out, “An e-mail may be considered hacktivism by some and some cyber terrorism by others”.\textsuperscript{165} In the form of cyber terrorism the terrorist, finds an easy, risk-free, low-cost option.\textsuperscript{166}

In 1997, Barry Collin coined the term “cyber terrorism” and defined it as the convergence of cybercrime and terrorism.\textsuperscript{167} The term has since entered popular parlance and is also defined as “attacking sabotage prone targets by computer, which poses disastrous consequences for our incredibly computer-dependent society’.

\textsuperscript{163}Peter Stephenson: Investigating Computer Related Crime p.85.
\textsuperscript{165}Talat Fatima: Cybercrimes, 1st Edn. 2011 Eastern Book Company, p-196.
\textsuperscript{166}Ibid.
Cyber terrorism falls in the taxonomy of cybercrimes as like cybercrimes, it is the misuse of computer technology. Cybercrimes are usually single-handed acts while cyber terrorism is a chain of acts committed by organized terrorist groups.

**Red Fort Attack Case (2000):**

On December 22, 2000 at about 9 p.m. in the evening some intruders started indiscriminate firing and gunned down three army Jawans belonging to 7th Rajputana Rifles. The Quick Reaction team of the battalion returned the firing towards the intruders who escaped by scaling over the rear side boundary wall of the Red Fort. This attack rocked the whole nation generally and the city of Delhi in particular.

The facts of case Mohd. Arif @ Asfaq v. State of NCT of Delhi prove beyond doubt that there were used several mobile phones and a computer centre called Knowledge Plus run by the appellant Arif alias Ashfaq, in the process. It may be mentioned that Arif was a Pakistani national but had fraudulently got a ration card, landline phone, cell phone, driving licence, and even a flat in Delhi in his name in Delhi in order to play his role in executing the terrorists’ plan of attacking the historic monument Red Fort.

In the light of the provisions of IT Act, as amended in 2008, this could be termed as a case of cyber terrorism; but in the absence of the same, the accused person were tried under the relevant provisions of Indian Penal Code, 1860. Confirming his death sentence, the apex Court made the following observations:

---

…In fact, this is a unique case where there is one most aggravating circumstances that it was a direct attack on the unity, integrity and sovereignty of India by foreigners. Thus, it was an attack on Mother India. This is apart from the fact that as many as three persons had lost their lives. The conspirators had no placed in India. Appellant was a foreign national and had entered India without any authorization or even justification. This is apart from the fact that appellant built up a conspiracy by practicing deceit and committing various other offences in furtherance of the conspiracy to wage war against India as also to commit murders by launching an unprovoked attack on the soldiers of Indian Army. We, therefore, have no doubts that death sentence was the only sentence in the peculiar circumstance of this case.

We, therefore, confirm the judgment of the trial Court and the High Court convicting the accused and awarding death sentence for the offences under Section 302, Indian penal Code, 1860. We also confirm all the other sentences on all other counts and dismiss these appeals. (Emphasis added.) Laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13, 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents. The laptop contained several evidences that confirmed of the two terrorists motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully scanned and the seal was also craftly made along
with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

0. Judicial Response on E-Mail Misuse:

Electronic mail properly called as e-mail has become most popular and convenient mode of communication. It has, however, serious limitations. It can be intercepted and modified, changed or altogether altered by the interloper. The changes thus made cannot be detected. The sender of the mail can hide his identity. Technologically it is possible to make an e-mail appear to have come from third person. This flexibility in communication has paved the way for e-mail misuse. Nowadays, e-mails are being used to perpetrate frauds, scams, terrorist activities and other heinous crimes. A good number of cases have been decided in America pertaining to e-mail abuse.

In United States v. Kammersell,169 the defendant was found to have sent a threatening e-mail via AOL an interstate service. It was held that federal interstate jurisdiction was proper even though the message was sent from and received in the same state.

It was further held that federal laws prohibiting transmission in interstate commerce of communications containing threats applied, because the e-mail was sent via a commercial online service and routed outside the state before reaching its final destination within the state.

In United States v. Machado,170 the defendant had sent threatening e-mail to Asian students at University of California at Irvine based on race/ethnicity. The defendant contended that the e-mails were sent idly and without intention to act on threats. The court, however, did

170 C.D. Cal. 2/10/98 USA
not accept his contention and held accused liable for violating federal hate-crime law.

In State of Washington v. Townsend,\textsuperscript{171} a Washington Appellate Court affirmed a conviction for second degree rape of a child. The defendant appealed the lower court’s decision to admit into evidence copies of e-mail messages between himself and a police officer posing as a 13 years’ old girl. The defendant argued that the e-mail messages were copied in violation of the Washington privacy Act, which prohibits the copying of private communications transmitted by telephone, telegraph, radio or other device.

p. Judicial Response on Data Theft:

According to Wikipedia Data Theft is a growing problem primarily perpetrated by office workers with access to technology such as desktop computers and hand-hold devices capable of storing digital information such as flash drives, iPods and even digital cameras. The damage caused by data theft can be considerable with today’s ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices.

T-Mobile Data Theft Case\textsuperscript{172} is a landmark case of Data Theft. The Chester Crown Court has orders two former employees of UK mobile operator T-Mobile to pay a total of $73,700 after stealing and selling customer data from the company in 2008. It is a landmark ruling because, it is a record fine for data protection offences, but more important than that, is that for the very first time we are seeing the criminal courts taking data protection seriously, David Turley and Darren

\textsuperscript{171} No. 19304-7-111 (Wash. Ct. App. 2001) USA
\textsuperscript{172} June 2011 Chester Crown Court (UK).
Hames pleaded guilty to offence under Section 55 of the Data Protection Act, but the fines were imposed under the Proceeds of Crime Act. Mr. Turley was ordered to pay $45,000 and Mr. Hames was ordered to pay $28,700. Both face an 18-month prison term if they fail to pay within six months.

The IT Act, 2000 as amended by IT (Amendment) Act, 2008, Section 43(b) read with Section 66 is applicable and under Section 379,405 & 420 of Indian Penal Code, 1860 is also applicable with data theft.

In *Just Dial v. Infomedia 18 Delhi HC*,173 Just Dial, with a single national number 69999999 in 240 cities, has obtained injunction against Infomedia 18 Limited (one of the group company of media group TV 18), restraining it from carrying out any business or rendering any service of providing information of business, services, and products, through their newly launched website askme.in.

In a suit filed by Just Dial against Infomedia 18, Just Dial alleged that Infomedia 18 had copied its extensive database and was displaying the same on its website askme.in, thereby infringing Just Dial’s copyright in its valuable database. The Delhi High Court has granted an exparte injunction against Infomedia 18, restraining them from infringing Just Dial’s copyright and from running the website askme.in till the next date of hearing. The High Court has also appointed commissioners to visit Infomedia 18 Ltd,’s office in Delhi and Mumbai and to seize and take into custody all the CPUs, compact,


{363}
floppy discs and/or other storage media containing any part of the commercial or business directory database belonging to Just Dial.

q. Judicial Response on Illegal Online Selling:

It is becoming increasingly common to find cases where sale of illegal articles such as counterfeit currency, counterfeit branded products, narcotics drugs, weapons, wildlife etc. is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc. It is practically impossible to control or prevent a criminal from setting up a website to transact in illegal articles. Additionally, there are several online payment gateways that can transfer money around the world at the click of a button. The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claims.

In Sanjay Kumar Kedia v. Narcotics Control Bureau, the Supreme Court deciding a special leave petition touched on Section 79 of the Information Technology Act, 2000. The Petitioner (Sanjay Kumar kedia) was ostensibly running an online pharmacy which was alleged used to sell psychotropic substances to customers without prescriptions. He was subsequently issued a notice Section 67 of the Narcotic Drugs and Psychotropic Substances Act, 1985. Thereafter the petitioner filed an application for bail several times which was rejected by the courts and hence preferred the special leave petition to appeal against the orders for refusal of bail. The counsel for petitioner cited section 79 as a defense stating that it granted immunity from prosecution. He stated that the companies of the petitioner only provided third party data and

174 Decided by Supreme Court on December 4, 2007.
information without any knowledge as to commission of an offence under the Act. The respondents (Narcotics Control Bureau) rebutted this by stating that the petitioner and its associates are not an intermediary as defined under section 79 of the said Act as their acts and deeds was not simply restricted to provision of third party data or information without having knowledge as to commission of offence under the NDPS Act. The company (Xponse Technologies Ltd. And Xpose IT Services Pvt. Ltd headed by Sanjay Kedia) has designed, developed, hosted the pharmaceutical websites and was using these websites, huge quantity of psychotropic substances (Phentermine and Butalbital) have been distributed in USA with the help of his associates. The Supreme Court quite correctly applying the law as its stands held that (a) the petitioner was not an innocent intermediary as defined under Section 79 of the Technology Act according to the investigating agencies, they were the owners and were responsible for the contents therein; and (b) Section 79 will grant immunity to an accused who has violated the provisions of the Information Technology Act, 2000 and not grant an immunity under the Narcotics Drugs and Psychotropic Substances Act, 1985.

r. Judicial Response on Email Spoofing:

According to Wikipedia e-mail spoofing is e-mail activity in which the sender addresses and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. e-mail spoofing is sending an e-mail to another person so that it appears that the e-mail was sent by someone else.

Under the IT Act, 2000 as amended by ITAA, 2008, Section 66-D is applicable and Sections 417, 419 and 465 of Indian Penal Code, 1860 are applicable.
Pranab Mitra, former executive of Gujarat Ambuja Cement impersonating himself as a woman, Rita Basu created a fake e-mail ID through which he contacted Mr. V.R. Ninawe an Abu Dhabi businessmen. After long term relationship through interaction through email and other cyber medium, Mitra sent an emotional e-mail that "she would commit suicide" incase Ninawe ended the relationship. He also gave him "another friend Ruchira Sengupta's" e-mail ID which was in fact his second bogus address. When Ninawe mailed at the other ID he was shocked to learn that Mitra had died and police is searching Ninawe. Now Mitra faced the liability under the law and he has to spend huge amount to get out of the legal entangle. Finally however he went to Mumbai to lodge a complaint regarding the fact that he was in fact cheated by Pranab and he has no role in his murder.

s. Judicial Trend in Other Cases:

In Center for National Security Studies Vs U.S Department of Justice,\textsuperscript{175} the Circuit Court applied the mosaic theory to uphold the Justice Department’s categorical denial of FOIA requests for information about more than seven hundred people detained in the wake of the 9/11 attacks.

In North Jersey Media Group Vs Ashcroft,\textsuperscript{176} the third Court applied the theory to uphold government’s decision to close 9/11 “special interest deportation” hearings to the Public and Press.

In Alkhaz Case\textsuperscript{177}, an individual proficient with the use of a computer used the Internet to post a child's (or adult's) name and telephone number on sexual explicit Internet sites. This posting invited

\textsuperscript{175} 17 F.Supp.2d 58
\textsuperscript{176} 205 F.Supp. 2d 288, 300
\textsuperscript{177} 200 U.S. 113 (1993).
visitors to call and inquire about the named individual, who was a child. As a result, the named individual was subjected to consistent, harassing and possibly sexual explicit telephone calls every day of the week, at any and all hours. The repeated inquiries caused the recipient of the calls and/or messages to become fearful for his/her safety and the safety of their family. The Boehle family decided that they had to move outside of Will County in order to protect their daughter, who was the subject of the postings, telephone calls and messages, from any potential harm they feared might occur as a result of such harassment.\textsuperscript{178}

The Alkhaz case is one instance in which existing law proved to be inadequate to deal with computer-facilitated anti-social conduct. Other examples abound, some of which were ultimately addressed by the amendment of existing law or the adoption of new penal law.

In Basavraj R. Patil v. State of Karnataka,\textsuperscript{179} the point of law involved in the case was whether an accused needs to be physically present in Court to answer the questions put to him by the court whilst recording his statement under Section 313 of the Code of Criminal Procedure, 1973. If the world ‘personally’ used in the section is strictly and literally construed, it would mean that the accused has to be physically present in the court. This was the view held by minority Judges in this case but the majority judgment held that the provisions of Section 313 of Cr. P.C. have to be considered in the light of the revolutionary changes in technology of communication and transmission and the marked improvement in facilities for legal aid in the country.


\textsuperscript{179} AIR 2000 SC 3214
Therefore, it is not necessary that in all cases the accused must answer by personally remaining present in the court. Particularly, when evidence is being recorded by video-conferencing, the accused person may answer the questions put to him by court on the screen, and it will be as good as his personal physical presence in the court.

In S. Sekar v. The Principal General Manager (Telecom) (S.S.N.L.), the petitioner is an employee of the second respondent, B.S.N.L., working as a Telecom Technical Assistant (Switch). It so happened that while he was working in SIPCOT MBM Main Exchange, Keeranur, the B.S.N.L. higher officials suspected him and others for having committed offences in manipulating the computer system and thereby causing loss to B.S.N.L. The FIR in Crime No. 1 of 2004 was come to be registered on 06.01.2004 by the Police, Pudukottai, for the offence under Section 406, 420 and 468 I.P.C. and 43(g) of the Information Technology Act, 2000.

The main trust of the grievance of the petitioner in this case is that when there is a special enactment namely, the Information Technology Act, 2000 which is an operation relating to the alleged misconduct attributed as against the petitioner, there is no question of invoking the penal sections under the Indian Penal Code, It is also his specific plausible argument that Section 43(g) of the Information Technology Act, 2000, has been invoked without any basis. The Second respondent filed the computer which was adopted by the first respondent also, denying and refuting the allegations and the averments highlights that the FIR registered was proper and the Police is investigating into the matter properly.

The point for consideration is as to whether FIR referred to supra, has to be declared null and void as prayed by the Writ petitioner?

It was held that the Police to investigate thoroughly into the matter and add or delete the penal Sections under the Information Technology Act, 2000, as well as IPC and ultimately, it is for the criminal court which would be seized of the matter to decide on that. The Section 43(g) of the Information Technology Act, 2000, invoked by the police and specified in the FIR is declared void. Accordingly, the Writ petition is ordered. No cost, connected M.P. is closed.

In Kalyan Chandra Sarkar Vs Pappu Yadav, Pappu Yadav was arrested for murder and was imprisoned in the Belur jail at the state of Bihar. Pappu Yadav flagrantly violated all the norms envisaged in the jail manual and he entertained a large number of guests from outside and went to the extent of humiliating the Inspector General of Police boastfully on the ground that since he is a political person his whims and caprice would prevail. Hence it led to a hue and cry and it was almost going to be settled for once and all that he should be transferred out of Bihar so that the trial could take place without fear and favour from the political parties. However the defense lawyer contended that once it is going to be materialized then it is going to vitiate the ends of justice as he will not be able to attend the court proceedings and instruct the counsel effectively. The Court placing reliance on the Praful Desai judgment held that even if he is not transferred out of Bihar and is not physically present in the Court room the trial can be held with the help of video conferencing.

181 2004 7 SCC 539

{369}
In *Maharashtra Vs Praful Desai*,\(^{182}\) the Supreme Court examined the question regarding use of modern technology like recording of evidence by way of video conferencing at length. In the said case, interpretation of section 273 Cr.P.C., which requires that evidence in a trial has be taken "in the presence of the accused" or his pleader, came up for consideration. In that case, the prosecution wanted to record evidence of a doctor in US through video conferencing, as the doctor refused to come to India for deposing evidence and there was no way by which presence of the said doctor could have been procured by our courts. The Supreme Court held that recording of evidence by use of videoconference satisfied the requirement of section 273 Cr. P. C.

*Nirav Navinbhai Shah & 4 ors. V. State of Gujarat and Anr.*\(^ {183} \):

**Conclusion**

A critical evaluation of the case-law referred to above, makes it abundantly clear that operation of global networks and the concept of quasi-physical territory associated with cyberspace, call upon the need for a new legal perspective and pragmatic approach in handling cyber related crimes by the judiciary. With the tremendous growth of e-commerce, e-banking and e-service regime, the law applicable and administered to cyberspace crimes should be in tune with legal requirements for avoiding the vagaries and discrepancies of national administration of justice system, be it criminal or civil.

There has been significant change in the judicial trend with regard to adjudication of cybercrime during the past two decades. Realising the

---

\(^{182}\)Appeal (crl.) 476 of 2003 Appeal (crl.) 477 of 2003

fact that data stored, processed and transmitted in the electronic form is not directly tangible; the courts while adjudicating on cyber cases no longer adhere to strictly rigid and literal interpretation of law but adopt a more pragmatic and practical approach to the problems involved in the case before them for disposal, without, however, deviating from the basic intent of the legislature in enacting the law applicable to the case.

In view of the expanding dimensions of cybercrimes in India in recent years, it is not only the police force but also the judicial officers at the lower as well as higher level, who need to be properly educated and trained in various technological aspects of cybercrimes. In the present scenario, the perpetrators of these crimes are moving much faster than the law enforcement agencies in exercising effective control over them. The need of the time therefore, is that the judiciary should move faster than the law enforcement agencies in exercising effective control over them. The need of the time therefore, is that the judiciary should move faster than the cyber criminals by expediting disposal of cyber cases within a time-frame and make sure that the guilty do not escape punishment due to vagaries of law and evidence. As it has been rightly said, “the threat at present is not from the intelligence of the cyber criminals but it is from the ignorance and lack of will to fight against cyber criminality”. It may be reiterated that computer is a tool as well as a target for the preparation of cybercrime. The Information technology Act, 2000 specifies the illegal acts which have been made punishable as offences under the Act. The amendments made in the Indian Penal Code, law of Evidence and Criminal Procedure, Banker’s Book Act and the Negotiable Instruments Act also enable the law enforcement agencies and the judiciary to nab cyber criminals promptly and punish them.
The statistical data of cybercrime in India indicates that the incidents of these crime is constantly on an increase as compared to the rate of conviction which is significantly low the reason being that there is general lack of awareness about the computer crimes among the people who at times even do not know that they have fallen a victim to the illegal activities of perpetrators of cybercrime. In result, most of the crime remain unreported, and a few which are reported, result in acquittal due to ignorance of the police and investigating officials about the technicalities of these crimes and lack of sufficient evidence against the accused.\textsuperscript{184}

Realising the problem to and handicaps of the police, law enforcement agencies and prosecutors in handling cybercrime investigation due to inadequate knowledge and skill in this hi-tech field, Justice Yad Ram Meena, the Chief Justice of Gujarat High Court suggested that a forensic science University be set up in the State which will help the investigating officials and the judges to unravel vital clues in solving cybercrimes, economic offences and crimes committed by using sophisticated technology. It would also help in speeding up judicial proceedings. The conduct of judicial trial by video-conferencing has already commenced in major cities in India, which will gradually pick up momentum with the necessary infrastructure and equipment facilities being made available in court-rooms, police stations, prisons and lawyer’s chambers. Recourse to video-conferencing and similar new technologies will develop the law enforcement’s capability to stay abreast new cybercrimes such as encryption etc. and it will go a long way in improving the quality of justice particularly, in reducing costs and delays in disposal of cases specially, the computer related offences.

\textsuperscript{184} Rohas Nagpal: Seven Years of Indian Cyber Law, paper presented in Clubhack in December, 2007.
One of the cyber law experts and Supreme Court lawyer Mr. Pawan Duggal has suggested that there is urgent need for special tribunals being set up headed by well equipped and properly trained Judges to deal solely with cybercrime cases. 185 Another cyber law specialist Shri Prathmesh Popat practicing in Mumbai has underlined the need for computer friendly lawyers and Judges who are well versed with the functioning of the computer system and its operational pitfalls to handle cybercrime cases.