CHAPTER-V

Cyber Crime : The Judicial Endeavour

The outpouring of cyber crime cases in India has opened a new edge of challenges for law enforcement agencies. The growth of Information Technology has put real people beyond the physical boundaries in entirety. It is true to say that every coin has two sides. The new digital global village, which has came into existence with a lighting speed, is with endless benefits as well as downsides.

The criminal justice system in India has attained maturity over a period of more than a century and half and has earned international reputation as one of the efficient judicial systems of the world. The vital agencies concerned with administration of criminal justice include the 'Parliament (law-makers), the police (law enforcers), the prosecutors, lawyers and the judges. They enjoy considerable functional freedom yet their working having been based on the principle of checks and balances, restrains them from encroaching upon each other's domain and act with complete co-ordination.¹

**Challenges before the Judiciary**

With the emergence of computer networks and internet, online culture has become an integral part of modern existence as most of our activities such as commerce, industries, banking, exchange of money, information communication, governmental and non-governmental official transactions, academic pursuits etc. are carried on through the internet. The position today is that whatever a person wants to know or see, he can have it on internet. But despite this brighter side of the computer technology, there are certain negative aspects which are a serious cause of concern not only for the law-enforcement agencies but the judicial functionaries as well. The internet culture in its wake, has given rise to a number of online disputes, differences, controversies etc. resulting out of misuse of abuse of computer networks for illegal activities. Though disputes as such are not new to human society a they are known to have existed ever since the dawn of human civilization but the perturbing factor is that disputes relating to online transactions are entirely different 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 intricacies 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 recognise geographical or territorial boundaries;

(ii) Variation in the legal systems and laws and procedure of different countries as regards admissibility of cyber-related cases; and,

(iii) 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 involving cybercrime.

Commenting on the problems 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,\(^2\) 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

\(^2\) AIR 2006 SC 2820 (Para 11)
scientific expertise or not have the sufficient insight to tackle with the new situation. 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 punishments for them, does not deal with all problems which are faced by the officers enforcing the Act."

**Judicial Sentencing : Trend**

A cursory glance at the judicial administration in the Indian setting would reveal 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 is committed and its effect 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 grounds for leniency in sentencing while recidivism, persistent association with criminals or criminal world as also the gravity or seriousness of the crime, attract severe punishment. However, these are mere generalizations and do not in any way fetter judicial discretion in sentencing the criminals. The Judges while considering the punishment can hardly afford to overlook the overall impact of crime on society as a
whole. Court's decision therefore, play a vital role in deciding a future
course of action in similar cases.\(^3\)

Although the case law available on cybercrime is far more scanty
as compared with the traditional crimes, it is constantly escalating 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 potential danger to society and therefore, they are
reluctant in mitigating the sentence of such offenders.

Expressing his views about judicial sentencing Leon Radzinovicz
observed that it may be justified to award a severe and exceptionally
lengthy sentence on grounds of dangerousness of the crime or a lighter
one for reformation of the offender, but a sentence out of all proportions
to the crime is repugnant.\(^4\) Since cybercrimes are more damaging, the
general trend is to award a severe punishment. The core question in the
context of cybercrime is whether it is the protection of society or the
prevention of crime which should gain primacy in awarding of the
sentence. However, in the absence of any specific criterion in his regard
the general trend seems to be in favour of prevention and control of
cybercrime by adopting a stringent view in sentencing of cyber offenders.
The case-law referred to in the succeeding pages reflects the response of

---

\(^3\) Paranjape N.V. (Dr.): Criminology and Penology (13th ed.) page 246-47
judiciary and its approach to resolve the cyber disputes by providing remedial relief to the victims of such crimes.

**Judicial Trend 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 Agency v. Union of India and others,

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 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

---

5 AIR 2006 All 23 (decided on 24.09.2006).
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 deemed 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) the 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.

**Cyber Pornography : Judicial Trend**

With the increasing use of internet in human life, there is preponderance of pornographic material on the web which has harmful effect not only on children and young persons but on society as a whole. In general terms, pornography may be said to be a predominantly sexually
explicit material that is intended primarily for the purpose of arousal of sex desire.

The main reason for rising incidence of pornography as a cybercrime appears to be that there is no regulation worth the name to restrict or regulate as to the type of persons who are permitted to access the internet. In India, the Videsh Sanchar Nigam Limited (VSNL) and a number of other private Internet Service Providers (ISP’s) provide internet access through different schemes but there is no restriction on the nature of persons permitted to avail of the internet service.

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,6 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 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 divorcee 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

---

6 Decided by the Chief Metropolitan Magistrae, Egmore, on November 5, 2004.
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 cafe 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 the case of Avnish Bajaj v. State (NCT Delhi), Baazee.com was an online auction website and Avnish Bajaj was its 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 with 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.

7 (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 week-end. 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 the accused deserved to be released on bail 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 the condition that he shall participate and assist in the investigation.
In Fatima Riswana v. State Represented by ACP, Chennai and others, 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 Sections 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 376, 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

8 Criminal Appeal 63 of 2005 arising out of SLP (Cri) No. 1606 of 2004 decided by the Supreme Court on January 11, 2005.
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 of creating Mahila Courts, as also the earlier decision\(^9\) 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 her 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.

In Air Force Bal Bharti School, Delhi case, a student of this school was teased by all his classmates for having a pockmarked face. Fed up with the cruel jokes, he decided to get back at his tormentors. He set up a web-side with pornographic material and scanned photographs of his classmates and teachers and morphed them with nude photographs and put them on the websites that he uploaded on to a free web hoisting service. The father of one of the class girls who happened to see the website objected to this and lodged a complaint with the Delhi Police. The School issued a show cause notice asking the boy as to why he should not be rusticated from the school for his pornographic offence. The case was taken up by the Juvenile Welfare Board which heard both the parties i.e. the counsel for the school and the counsel representing the girl's, father (complainant) and tried to compromise the matter but the father of the accused boy did not agree to withdraw the boy from the school until the school gave a written guarantee that his son will get admission in some other school, which the school and the Directorate of

---

Education were unable to give. The father of the girl (complainant) insisted that the matter would not be compromised so long as the accused boy is continuing in the same school as the parent of 12 children whose names and photographs were scanned in the web-site, did not want their children to study with the boy (accused) who could indulge in such a heinous crime. The defence allegation that even before the boy had set up the website other students had been sending objectionable e-mails about the teachers of the school through the school's internet connection, was not acceptable as the school produced sufficient evidence that it had no internet connection before April 4, 2001 i.e. the day accused was indicted for the offence of cyber pornography. However, the case was later dropped since it was compromised between the parties i.e. the School and the complainant.

In another case, a Swiss couple\textsuperscript{11} 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 Sections 292 and 509, IPC. But they were later let off for want of sufficient evidence against them.

\textsuperscript{11} Swiss couple cyber pornography case, Mumbai 2003.
In an American case, namely, United States v. Kufrovich, the accused was charged of an offence under Section, 2422 (b) and 2423 (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.

It is heartening to note that the High Court of Bombay in a suo motu writ petition (No. 1611 of 2001) appointed a Committee to recommend measures to protect and shield minors from pornographic and obscene material on the internet. Two activists Jayesh and Sunil Thakkar wrote a letter to the Hon'ble Chief Justice of the Bombay High Court complaining about the proliferation of pornographic sites on the internet. The Court treated the letter as suo motu writ petition. During the hearing of the said petition, the Internet Users Association of India (IUAI) was permitted to intervene in the matter and the Government of Maharashtra and the Union of India also appeared before the Court.

The Division Bench of the Court presided by Chief Justice passed an order dated September 28, 2001, appointing a High Court Committee\textsuperscript{13} to suggest and recommend ways, measures and means to protect minors from access to pornographic obscene material on the internet. The Committee made separate regulatory recommendations for internet service providers (ISP’s), cyber cafes and their licensing etc. It also recommended that every visitor to cyber cafe be required to produce photo ID card and suggested mandatory provisions for protective software and emphasised the need for co-ordination between ISP Association of India and CCIC.

**Judicial concern for IPR\textsuperscript{14} related Cybercrimes**

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

\textsuperscript{13} Mrs.. Archana Tyagi, DCP Enforcement was appointed as Chairperson of the Committee and Dr. Sourav Dutta of VSNL and Shri Vijay Mukhi of I.U.A.I along with Advocate Shashi Kumar Nair were its members. The Committee submitted its report to the High Court on January 30, 2002.

\textsuperscript{14} Intellectual Property Rights are referred to as ‘IPR’.

248
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 the case of Kirloskar Disel Reconstruction (P) Ltd. V. Kirloskar
Proprietary Ltd.\(^\text{15}\) the High Court of Bombay, held that the definition of
trademark includes within it the word 'mark', which means name and
therefore, the term 'trademark' in Section 105(c) of the Trademarks Act
must be considered to be 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

\(^{15}\) AIR 1996 Born. 149.
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 lie in cases of trademark or trade name violation. The defendant was therefore, restrained from using the name 'kirloskar' in their online advertisements and internet communications.

In the landmark case of Rediff Communication Ltd. v. Cyberbooth and Another. the plaintiff Rediff Communication Ltd. was a online media company which was carrying on the business of communication and providing internet service since 6th January, 1997. The word REDIFF comprised the first six letters of a group of companies having corporate names as Rediffussion, Denstu Young and Rubicam advertising Ltd. The plaintiffs got their domain name REDIFF.Com registered with the NetWork Solutions Inc. on February 8, 1997 and claimed to have a large turnover of Rs. 1.93 crores during the preceding years. It was in March 1997 that the plaintiffs learnt that defendants got their domain name RADIFF.COM registered with Network Solution Inc. on January 31, 1999 and had established webpage on the internet with the said domain name. The plaintiffs alleged that the adopting of the said domain name by the defendants was clearly intended to cause members of the

16 AIR 2008 Bom.27 decided by the Bombay High Court on April 23, 2008.
public to believe that the defendants are associated with the plaintiff or part of the 'Rediffusion Group' with whom the name mark 'REDDIFF' is exclusively associated and therefore, it was an act of passing off on the part of the defendants for which an injunction be granted by the Court. In other words, the defendants had deliberately passed off their business, goods, services etc. as those of the plaintiff's, and thereby illegally exploited the reputation and goodwill of the plaintiffs.

The defendants in their written statement supported by an affidavit contended that the word RADIFF adopted by them was coined by taking first three letters of the word 'Radical', the first letter of the work 'information', the first letter of the word 'future' and the first letter of the word 'free'. They further argued that there was no likelihood of deception or confusion as the two domain names 'REDDIFF' and 'RADIFF' were distinctly different and also that the plaintiff's website was titled 'REDDIFF' on the internet whereas defendant's website was titled as 'RADIFF ONLINE'. Further, the plaintiffs' website was providing various services from news to shopping whereas the defendant's website was mainly providing hyper text links' to its advertiser's websites. Thus the look and feel of the plaintiff's website was totally different from that of the defendant's website.
Analysing the principles underlying the law relating to passing off, Mr. Justice A.P. Shah of the Bombay High Court (as he then was) referred to Lord Diplock's observation in Erven Warinick v. Townend\textsuperscript{17} case wherein it was held that the essential characteristics which must be present for a valid passing off action are: (1) misrepresentation, (2) made by a person in the course of trade or business, (3) to the prospective customers of goods or services supplied by him, (4) which is calculated to injure the goodwill of another trader as a foreseeable consequence; and (5) which causes actual damage to the business or goodwill of the trader by whom action is brought against the defendant.

The High Court of Bombay came to the conclusion that when both the domain names are considered, it is clearly seen that they are almost similar in nature and there is every possibility of internet users being confused and deceived in believing both the domain name belong to same person although in fact the two belong to different persons. Rejecting the defendant's plea that the word RADIFF was derived from the four words, namely 'radical' information', 'future' and 'free', the Court held that this assertion appears to be completely false and an afterthought devised to answer the plaintiff's claim. The Court concluded in unequivocal terms that the prima facie object of the defendant in adopting RADIFF as a domain name was to trade upon the reputation and goodwill of the trader.

\textsuperscript{17} (1979) 2 All ER. 927.
plaintiffs domain name and the argument that the field of activity of the
two was different is without any substance because both activities are
similar as also overlapping. The defendant was therefore, restrained from
using the domain name RADIFF forthwith.

In the case of TATA & Sons v. A.K. Chaudhary,\textsuperscript{18} the petitioners
used TATA logo in its website for its products. They sued the defendant
for openly selling his steel and cutlury and similar items using
deeperly 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.

The Supreme Court in M/s Satyam Infoway Ltd. v. M/s Sifynet
Solutions Pvt. Ltd.\textsuperscript{19} held that domain name used as a mode of carrying
on commercial activity has all the characteristic of a trademark, it is not
merely an address on internet but serves as a business identifier as it
identifies and distinguishes, goods or services made available to internet

\textsuperscript{18} 2009 (40) PTC 54 (Del.)
\textsuperscript{19} AIR 2004 SC 3540.
users. Bringing out a distinction between trademark and domain name, the Apex Court held that the distinction lies in the manner in which the two operate. A trademark is protected by laws of the country where such trademark is registered. Consequently, a trademark may have multiple registration in many countries. As against this, a domain name is potentially accessible without any geographical location of the consumers. Although there is no specific legislation in India which explicitly refers to dispute resolution in connection with domain names but that does not mean that domain names are not to be legally protected. They, are adequately protected by the law relating to passing off action under the law of torts.

In an action for passing off as the term itself suggests, the defendant tries to pass off his goods or services to the consumers or public as that of the plaintiff’s goods or services. It is an action not only to preserve the reputation of the plaintiff but also to safeguard public or customers against confusion or deception. The similarity of domain names in e-commerce with its instant accessibility may result in users mistakenly accessing one domain name for the other due to similarity of both the names.

In the instant case, the appellant was an incorporated company registered in 1999 under several domain names like www.sifynet.com, www.sifymall.com, www.sifyrealestste.com etc. with the internationally
recognised Registrars, namely, Internet Corporation for Assigned Names and Numbers (ICANN) and the World Intellectual Property Organisation (WIPO). The word 'sify' was coined by using elements of its corporate name, Satyam Infoway and the appellant claimed a wide reputation and goodwill in its name 'sify'.

The respondent started carrying on business of internet marketing under the domain names 'www.siffynet.net' and 'www.sifynet.com' from June 2001 which were registered with ICANN on 5th June, 2001 and 16th May, 2002 respectively. Having come to know about the use of domain name 'sify' by the respondent, the appellant served a notice on the defendant asking him to desist from using that domain name as it was deceptively similar to that of the company's domain name, but the defendant refused to oblige. Consequently, the appellant filed a suit against the defendant in the City Civil Court claiming passing off action against the latter and an application for temporary injunction against the defendant. The Court granted injunction on the ground that the appellant was the prior user of domain name 'sify' which had earned considerable reputation in connection with internet and computer services therefore, adoption of similar domain name by the defendant was deceptive and likely to cause confusion among the users and the customers.
The respondent preferred an appeal against the Civil Court's order in the High Court which stayed the injunction order and later allowed the appeal on the ground that merely because the appellant had started the business first, did not entitle him for an injunction without considering as to where the balance of convenience lay. The Court in this case noted that, the record showed that respondent was carrying on business other than that of the plaintiffs and there being no similarity between the two businesses, there was no question of customers being deceived or confused. The claim of appellant was therefore, disallowed by the High Court.

In Himalaya Drug Co. v. Summitt\textsuperscript{20} 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 synthactical and grammatical form that appeared on the appellant's website was copied verbatim by the defendant in their website. The appellants, therefore, moved the Delhi High Court for an injunction

\textsuperscript{20} 2006 (32) PTC (Del).
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.

In yet another case, namely Dalgit Titus, Advocate and others v. Alfred A. Adevare and others21 decided by the Delhi High Court, the plaintiffs were running a law firm which consisted of advocates specialised in different legal fields. The defendants were working with the plaintiff's firm and were paid remuneration while they retained control over the professional organisation. They claimed copyright ownership 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 plaintiff's firm, they could not claim exclusive right in respect of database of the list of clients and the

21 2006 (32) PTC 609 (Del).
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 plaintiffs 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 copyright 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, utilise 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 clauses 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.\textsuperscript{22}

The American case of Marks and Spencer PLC v. One in million\textsuperscript{23}, may also be cited wherein it was held that any person who deliberately registers a domain name on account of its similarity to the name, brand name or trademark of an unconnected commercial organisation, may be restrained from such passing off activity by an injunction. The defendants in this case adopted the name Marks and Spencer domain name only because this name was associated with the plaintiff's group which had good business and the defendant wanted to use it illegally for his own gain by causing confusion or deception among the users or customers.

Where the controversy between the parties centers around the domain name on the internet, the principle laid down in the landmark case of American Civil Liberties Union (ACLU) v. Reno\textsuperscript{24}, may be followed to arrive at a correct finding. In that case, Justice Mokenna inter-alia held that each host computer providing internet services (site) has a unique internet address. The users seeking to exchange digital information such as e-mails, computer programs, images, music-etc. with a particular internet host require the 'host' address in order to establish

\textsuperscript{22} Narayana on Copyright and Industrial Design (3rd ed.) paras 6 & 28.
\textsuperscript{23} 1998 FSR 265 (US).
connection. In fact, host actually possesses two addresses i.e. a numerical 'IP' address such as 125, 555, 600 and an alpha numeric "domain name" such as microsoft.com; sify.com. The internet domain names are similar to a telephone number but they are valuable corporate asset as they facilitate communication with a customer base. The uniqueness, of internet address is ensured by the registration services of the Internet Network Information Center. In USA, the National Service Foundation (NSF) which registers domain names free on 'first come first serve' basis. It does not determine the legality of domain name registration nor does it verify whether that domain name has already been registered earlier by someone and may lead to infringement of the right of prior owner of it. Anyone may apply for the domain name and if it is available, it could be allotted to him.

In an English case, namely, Erven Warnick v. Townend, Lord Diplock set out the essential requisites for an action against defendant for passing off where the dispute relates to adoption of domain name by the defendant similar to that of the plaintiffs domain name. They are:

1) there must be misrepresentation;

2) made by the defendant in course of his trade or business;

3) to his prospective consumers or ultimate consumer of goods or services, supplied by him;

25 (1980) RPC 31 (UK) : (1979) 2 All ER 927.
4) which is calculated to injure the business or goodwill of the plaintiff (i.e. another traders) ;

5) the consequences of which could have reasonably been foreseen by the defendant; and

6) such consequences do actually result in causing actual damage to the business or goodwill of the plaintiff.

From the above, it is evident that intent to deceive is not an essential requirement to prove the deception of the defendant. However, it would not be wholly immaterial as it may help the Court to draw inferences as to the motive of the defendant.26

The WIPO Administrative and Mediation Centre's decision in the arbitration case of Bennett Coleman & Co. Ltd. v. Steven S. Lalvani along with Bennett Coleman & Co. Ltd. v. Long Distance Telephone Company27 laid down certain principles of cyber law on domain name which may provide effective guidelines for the prevention of cyber squatting and the related crimes. These principles are:—

1) Daily usages of newspaper titles/marks in hard" copy or electronic publication leads to a substantial reputation which cannot be allowed to hijacked in cyberspace by a squatter.

27 Administrative Panel decision of Arbitration & Mediation Centre delivered by Panelist W.R. Cornish of the WIPO on March 11, 2000.
2) According to the principle of presumption, the moment anyone registers a domain name which has the trademark or other mark of any other entity, it shall be presumed that, the said person was fully aware of the existence of the said mark at the time when he applied for the registration of the domain name.

3) The website being a "postal address" to other sites, it will be presumed that the defendant is adopting domain name to take advantage of the good reputation of the plaintiffs domain name,

The facts of the case were that the complainant of Bennett Coleman & Co. Ltd. were the publishers of two reputed papers, namely, "The Economic Times", which had an average daily circulation of around 35 lakhs, and the "Times of India", which had a circulation of nearly 1.52 crores per day. Besides, they were carrying out publication of certain supplemental material using the brand name Times" and held domain names www.economictimes.com and www.timesofindia.com, using them for electronic publication of their respective aforesaid two newspapers.

The complainant had registered in India under the mark "The Economic Times" for newspapers, journals, magazines, books and other literary works on March 28,1973 and the mark "The Times of India" on July 30, 1943.
The defendant, Stevens S. Lalvani, a resident of Lipper Montclair, USA got the domain name www.economictimes.com registered with Network Solution (NSI). He also got the domain name www.thetimesofindia.com registered with NSI for his Long Distance Telephone Co. having the same address. Thereafter, Steven S. Lalvani and Long Distance Telephone Co., both built up websites of the two domain names with the result that any net users who legitimately wanted to go to the site of the Economic Times, when typed the same name in his browser, was redirected to the site of the defendant's website and thus resulted in great damage and harm to both the reputed publications of the plaintiff i.e. Bennett Coleman & Co. Ltd. This situation continued unabated until 1999 despite several notices and negotiations with the defendants but the latter did not mend his ways and continued his illegal activity of cyber squatting.  

During the closing decades of the 20th century, the practice of cyber squatting was a hot issue worldwide because of the fact that Network Solutions did not prescribe any restriction on the registration of domain names. However, perturbed by this growing menace, the U.S. Government established the Internet Corporation for Assigned Names and Numbers (ICANN) in 1999 which is now the global body for

---

28 Cyber squatting refers to a practice by means of which a person or legal entity gets registered the trademark, business name or service mark of another as his own domain name for the purpose of holding it on and thereafter selling the same domain name to other persons for valuable consideration or premium.
managing internet. ICANN has introduced a uniform Domain Name Dispute Resolution Policy which came into force with effect from December, 1999.

Taking advantage of the Uniform Domain Name Dispute Resolution Policy, the complainant Bennett Coleman & Co. Ltd. filed two cases against the defendants before the WIPO Arbitration and Mediation Centre on 27th January, 2000. Both the complaints being against the same defendants were taken together and were hotly contested by the defendant Steven S. Lalvani. The case was disposed of by the WIPO Arbitration Centre in favour of the plaintiff and the defendant was directed to transfer both the disputed domain names to the complainant.

Is ATM a computer? — Judicial View

A controversy that came up before the High Court of Karnataka in Diebold Systems Private Ltd. v. Commissioner of Commercial Taxes,\textsuperscript{29} for decision was related to the question whether Automatic Teller Machine (ATM) is computer? In this case, the appellants, Diebold Systems Pvt. Ltd. were the manufacturers and suppliers of Automatic Teller Machines (ATMs). They sought a clarification from the Advance Tax Ruling Authority (ATRA), Karnataka on the rate of tax applicable on sale of their products Automatic Teller Machines under the Karnataka

\textsuperscript{29} ILR 2005 Kant 221 (decided on January 31, 2005).
Sales Tax Act, 1957, the ATRA classified ATMs as 'computer terminals' liable for four basic taxes as they would fall under Entry 20 (ii)(b) of Part C of the Second Schedule of the Karnataka Sales Tax Act. The Commissioner of Commercial Taxes, on the other hand, was of the view that ATRA's ruling was erroneous and passed an order that ATMs cannot be classified as computer terminals as per Section 2 of the Information Technology Act, 2000. The matter was therefore, referred to the High Court of Karnataka for final decision. The Court held that ATMs are not computers; instead they are mere electronic devices for the purpose of imposition of taxes under the Karnataka Sales Tax Act. Giving reasons as to why ATM cannot be treated as computer, the Court held that an enlarged definition of computers in the Information Technology Act, 2000 cannot be extended for the purpose of interpreting or Entry under fiscal legislation. The Court observed that Automatic Teller Machine is an electronic device which allows a customer of the bank to make cash withdrawals and check his account balance at any time without the need of human teller. Therefore, it would be incorrect to call and ATM machine as computer by itself as it is connected to a computer that performs the tasks requested by the person using ATM. Many ATMs located at different places are electronically connected to a computer, as such they are only electronic devices and not themselves computers.
Need for developing Cyber Forensics: Judicial Approach

The term 'computer forensic' was coined for the first time by the International Association of Computer Specialists (IACS) in Oregon (USA) in the year 1991. 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 major areas," namely (i) computer forensics, (ii) cyber forensics, and (iii) software forensics.

Computer forensics deal with collection of evidence from the computer media seized at the scene of crime by extracting hidden or deleted information from the computer disk.

Cyber forensics is also called as network forensics and it deals with" analysis of digital or electronic evidence that is distributed across the large computer network. The main object of cyber forensics is discovery of evidence and assessment of the intent and identity of the perpetrator and to determine potential impact of criminal activity on the victim. This technique helps to find out whether the pertinent information
has been destroyed, modified or hidden deliberately, intentionally or incidentally with a view to causing harm to the victim.

Software forensics deals with the author of the malicious code. The key to identify the author of a suspect code is selection of appropriate body of code.

In Firoz. v. State of Kerala, the Court, inter-alia, observed that cyber forensics greatly help the investigators of cybercrime to prove the motive, means and opportunity for the criminal to commit the crime. That is, the purpose which prompted the perpetrator to commit the crime and means adopted by him, namely, why, how and when it was done. The motive may be anything from curiosity to money-making, revenge or misadventure.31

As stated above, cyber forensics mainly revolve round proceedings related to electronic records as evidence before a court of law. Electronic records have been given legal recognition under Section 4 of the Information Technology Act, 2000. The evidentiary value of a secure electronic record32 is more than any other electronic record because the burden of proof lies on the person who claims alteration of the electronic record. The electronic record produced before the court cannot ordinarily be substantiated by written or tangible material or human witnesses.

30 AIR 2006 Ker 279.
32 A secure electronic record as defined in Section 14 of the Information Technology Act, 2000 is one where any security procedure has been applied to an electronic record at a specific point of time.
Therefore, it has to be procured through cyber forensics which include discovery, analysis and reconstruction of evidence extracted from and/or contained in a computer, computer system, computer network, computer media or computer peripheral.

Forensic assistance is needed for finding out as to exactly what data was stored in a computer at the relevant time (i.e. at the time of perpetration of cybercrime). There are many types of information in a computer that are valuable from the point of evidence, which can be traced or found out through forensic procedure. The main among them include normal files, deleted files, hidden files, password protected information, data in free space, file slack, drive slack space etc.

The forensic method of examination of data stored in a computer is to ensure that the original evidence is not tempered with. This is possible by making minor images of the drives on the defendant's computers.

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\textsuperscript{33} 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, including files that had

\textsuperscript{33} 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.
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,\(^{34}\) 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 computer hardware to discover "purged" records. Similarly, Court has the power to appoint a neutral computer forensic expert to recover the deleted e-mails.\(^{35}\)

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

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

\(^{34}\) (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.

\(^{35}\) (1993) 839 F Supp. 1552 (U.S.)
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.

**Judicial trend in other cases**

The Supreme Court in M/s Satyam Infoway Ltd. v. Sifynet Solutions (Pvt.) Ltd.\(^{36}\) reiterated that the domain name used as a mode of carrying on commercial activity has also the characteristics of trademark. It is not a mere address on internet but serves as a business identifier-and therefore, passing off action may lie for the violation of domain name right.

In State of Maharashtra v. Praful B. Desai,\(^{37}\) the Supreme Court held that recording of evidence by video-conferencing in the presence of accused person is permissible under Section 273 of the Code of Criminal Procedure, 1973. Interpreting the words 'presence of the accused' used in this section, the Court clarified that the word 'presence' in the section does not mean actual physical presence in the Court, if the accused is present on the computer screen during video-conferencing, it will be as good a evidence admissible similar to actual physical presence of the accused in

---

\(^{36}\) AIR 2004 sc 3540 see also Acqua Minerals v. Promod Borse, AIR 2001 Del 463; Dr. Reddy's Laboratory v. Manu Kasuri, 2001 PTC 859 etc.

\(^{37}\) AIR 2003 SC 2053.
the Court of law. The facility of playback provides an additional facility in cross-examination of witnesses. The system of recording evidence by video-conferencing proves to be more advantageous where witnesses cannot be procured without delay, expense or inconvenience.

In the instant case, the complainant's wife was suffering from terminal cancer. The prosecution version was that the said lady was examined by Dr. Earnest Greenberg of Sloan Kettering Memorial Hospital, New York (USA) who had opined that she was inoperable and should be treated only with medication. Thereafter, the complainant and his ailing wife consulted the respondent who was a consulting Surgeon practicing for the last 40 years. In spite of being made aware of Dr. Greenberg's opinion, the respondent suggested surgery to remove the uterus of his ailing wife. She was operated by Dr. A.K. Mukherjee on December 22, 1987 but when he found that ascetic fluid was oozing out of the abdomen of the operated lady, he immediately closed the open stomach. Consequently, the patient had to remain in the hospital for more than three and half months and thereafter, she died. She required 20-25 dressings per day and suffered terrible physical torture and mental agony throughout the post operation period. The complainant sued the defendant alleging that the latter did not care to examine the patient even once after her operation. The respondent's claim that the complainant's wife was not his patient could not be relied because fee was charged by him for
operating the deceased. The complainant also brought to the notice of the Court that the Maharashtra Medical Council had held enquiry in the case and reprimanded the respondent for his negligent and guilty conduct as also issued a warning to him.

The respondent Dr. A.K. Mukherjee who was facing charges under Section 338 read with Sections 109 and 114, IPC, challenged the validity of the process against him but the Apex Court dismissed his special leave petition on July 8, 1996 and directed him to face the trail.

On June 29, 1998, the prosecution made an application to examine Dr. Greenberg through video-conferencing, which was allowed by the trial Court on August 16, 1999. The respondent challenged that order, hence the appeal came before the Supreme Court.

Dr. Greenberg had expressed his willingness to give evidence but had refused to come to India for that purpose. There being no provision to compel him to appear as a witness to give evidence before a Court in India, the Apex Court permitted the examination of Dr. Greenberg through video-conferencing, and rejected the plea of the respondents that there was no provision for examination of witnesses by video-conferencing in the Code of Criminal Procedure and that it will be in contravention of the provisions of Section 273 of Cr. P.C. which requires actual physical presence of the witness in the Court. The Court in this case observed:
"Video-conferencing is an advancement in science and technology which permits one to see, hear and talk with someone far away with the same facility and ease as if he is present before you. In fact he/she is present before you on a screen except for touching, one can see, hear and observe as if the party is in the same room. In video-conferencing both parties are in presence of each other. The submissions of the respondent's counsel are akin to an argument that a person seeing through binoculars or telescope is not in the presence of the person observing. Therefore, no prejudice of whatsoever nature is caused to the accused. However, evidence by video-conferencing has to be on condition that the equipment should have been set up in the Court itself so that evidence may be recorded under the directions of the Magistrate."

In case of a foreign witness, his evidence by video-conferencing should be recorded by the Court subject to two conditions, namely, (i) witness should be a national of a country which has an extradition treaty with India and under that country's law of contempt of Court; and (ii) perjury should be a punishable offence in that country. The fulfilment of these conditions will enable the Court to exercise jurisdiction in case the foreign witness commits any contempt of court or perjures himself.
In yet another case, namely, State of Punjab and others v. M/s Amritsar Beverages Ltd. and others, the question involved in the appeal before the Supreme Court was how far the situational change could give rise to a new interpretation of a statutory provision? The respondent in this appeal was a dealer whose premises were raided by the Sales Tax Department of Punjab State and a large number of books and documents in the form of cash books, ledgers or accounts registers were seized. A computer hard disk containing business information was also seized in the search conducted under Section 14(3) of the Punjab Sales Tax Act, 1948, the section required that such seized material had to be returned to the dealer within a period of 60 days from the date of seizure, after examination or extracts or copies thereof having been taken out.

The officials of the Sales Tax Department asked the respondent i.e. dealer to appear on several occasions so as to enable them to verify the contents and return the said documents to him but he did not turn up, hence documents could not be returned to him. He, thereafter, filed a writ petition requesting the Court to direct the Sales Tax Department to return the seized books, accounts, documents, computer disks etc. in terms of Section 14 of the Act. The High Court allowed the appeal directing the Sales Tax Department to return the seized documents of the dealer.

38 AIR 2006 SC 2820
alongwith the hard disk and also imposed costs of Rs. 2500/- for not having done so even after the expiry of prescribed period of limitation.

In compliance with the High Court's order, the Sales Tax Department returned the seized documents alongwith the hard disk but retained a copy thereof. The department asked the dealer to come to the Sales Tax office to verify the copy of the hard disk but he did not do so. In case of hard disk, literal compliance of the provisions of Section 14 was impossible without the dealer's co-operation in verifying the contents of the hard disc.

In appeal, the Supreme Court, set aside the High Court's order of award of costs for delay in return of documents by the Sales Tax Department in view of the fact that such computer related problem arose for the first time and therefore, a creative interpretation considering the circumstances and the development of science and technology was needed to meet the ends of justice. The Court directed the authorities of the Sales Tax Department to make out copies of hard disk and fix their signature and seal in physical form. The Court pointed out that, "internet and other information technologies have brought with them issues which were not foreseen by the law earlier. In view of the development of science and technology, the Court has to meet the challenges as an intermediary between the litigants".
The judiciary's anxiety for ensuring effective implementation and regulation of the Information Technology Act, 2000,\(^39\) as amended in 2002 and the rules framed thereunder is clearly discernible in the Bombay High Court's decision in the PIL writ petition filed by the students of the Asian School of Cyber Law located in Pune asking the Court for speedy appointment of Adjudicating Officers. Through this PIL, they had drawn the attention of the Court that Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000, which had come into force on October 17, 2000, provide for the appointment and working of the Adjudicating Officers and the Cyber Regulations Appellate Tribunal (salary, allowances and other terms for the presiding officer) Rules, 2003 which prescribe the salary, allowances etc. of the Presiding Officer came into force on March 17, 2003, but the Adjudicating Officers whose main responsibility under the Information Technology Act is to adjudicate cases such as unauthorised assess, unauthorised copying of data, spreading virus, Denial of Service Attacks (DoS), disruption of computers etc. have not yet been appointed by the Central Government. Expressing its anguish on this lethargic attitude of the Government in making the appointments of Adjudicating Officers and the Cyber Appellate Tribunals, the High Court of Bombay directed the Government to make the said appointments and notify it to the public through the media. The Court also ordered that the

\(^{39}\) The Information Technology Act came into force w.e.f. October 17,2000.
Cyber Regulation Appellate Tribunal be constituted within a reasonable time frame.

Consequent to the above directives of the High Court, the Central Government passed an order dated March 23, 2003 appointing the Secretary of the Department of Technology of each State or the Union Territory as the Adjudicating Officer.40

Taking a serious view as regards cases of online drug trafficking, the Supreme Court in Sanjay Kumar Kedia's case rejected his bail application for his company's involvement in booking online orders for prohibited drugs. Mr. Sanjay Kumar Kedia was the Business Processing Outsourcing (BPO) of the Information Technology Company. The Apex Court noted that Mr. Kedia though a highly qualified technologist heading two I.T. companies, namely, Xponse Technologies and Xponse I.T. Services was fully accountable for one of his company booking online orders for prohibited drug outside India for supply to customers abroad. He was arrested by the Narcotics Control Bureau (NCB) in February 2007. According to the Court, "appellant Kedia and his associates were not innocent intermediaries or network service providers as defined in Section 79 of the I.T. Act, but the said business was only a facade and camouflage for more sinister activities".

40 The Government also enforced the Information Technology (Security Procedure) Rules, 2004 w.e.f. October 29, 2004 providing security to digital signatures and electronic records.
41 A Bench of the Supreme Court comprising H.B. Sinha and H.S. Bedi, JJ. dismissed the bail petition of kedia on December 4, 2007.
The appellant had filed a bail application in the Supreme Court after the trial Court and the High Court had rejected his bail applications in April and June, 2007 respectively on the ground that sufficient time should be given to NCB to study the case as the alleged offence had "widespread ramification for society since it involved misuse of the cyber technology. The Apex Court upheld the bail rejection orders passed by the trial Court and the High Court and disallowed Kedia's bail petition on December 4, 2007.

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 cybercrimes during the past two decades. Realising the 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 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 perpetration 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\textsuperscript{42} 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{43}

Realising the problems 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 the 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

\textsuperscript{42} According to the National Crime Records Bureau (NCRB), the conviction rate for cybercrimes is only 10%.

\textsuperscript{43} Rohas Nagpal: Seven Years of Indian Cyber Law, paper presented in Clubhack in December, 2007.
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.

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. Another cyber law specialist Shri Prathmesh Popat practising 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.

The Supreme Court E-Committee

In view of the total pendency of cases as on September 30, 2009, around 29.5 million cases in subordinate Courts, about 38.42 lakh cases in High Courts and nearly 47364 cases in the Supreme Court, a National Policy and Action Plan has been launched in a phased manner to introduce information and communication technology in the Courts of

---

44 Pawan Duggal: Cyber Crime (2003) p. 154,
India which could be helpful in accelerating the judicial work and expeditious disposal of cases.

On the suggestion of Justice R.C. Lahoti, the former Chief Justice of India (CJI) the Union Government appointed a e-committee on December 28, 2004 under the Chairmanship of Justice Dr. G.C. Bharuka, a former Judge of the High Court of Karnataka with three other specialist members to formulate a National Policy on computerisation of the justice delivery system of India to be implemented in a phased manner.

The e-committee presented its report to the then CJI on November 5, 2005 after making consultations with legal and computer experts and internet service providers. The policy was proposed to be implemented in three phases during the ensuing five years.45

Phase-I extended to a period of two years and included the following reforms for modernisation of the judicial system in India:

(1) creation of computer rooms in all the 2500 courts of India;

(2) establishment of digital inter-connectivity between all District Courts with the Supreme Court;

(3) extending video-conferencing facilities at Supreme Court and all the High Courts and District Courts;

(4) equipping around 15000-judicial officers with laptops;

(5) extensive information and communication technology training to Judges and Court-staff;

(6) organising awareness programs and training modules for lawyers;

(7) creation of e-filing facility in Supreme Court and High Courts;

(8) development of integrated customised software application for judicial system with regional language support;

(9) digital presentation of under-trial prisoners and examination of witnesses and recording their evidence through video-conferencing.

Phase II of the National Policy on Information and Communication Technology (NICT) comprised:

(1) automation of registry level processes;

(2) digitilisation of law-libraries and court achieves;

(3) digital availability of case-law, statutory law and other legal literature;

(4) online availability of legal resources to judges, lawyers and clients;

and

(5) availability of e-mailing facilities at District and subordinate Courts.

The third and the last phase of NICT Policy, the duration of which was one year, was intended to ensure the use of bio-metrics and other hi-tech scientific tools and availability of information between courts,
prosecuting and investigating agencies, prisons, land-records and registration offices etc. with a view to expediting disposal of civil and criminal cases.

The National e-Courts Project for extensive computerisation of courts was launched by Dr. A.P.J. Abdul Kalam, then President of India on July 9, 2007 in New Delhi in the presence of CJI, Union Law Minister and other dignitaries including Judges of the Supreme Court and some of the High Courts. The President; expresses his vision to create-e-Judiciary and e-governance grid covering the entire Indian judicial system, which according to him, "will ensure transparency, speed and equity in the decision-making process".

Undoubtedly, these developments have greatly benefited all the repositories to the judicial system of India including litigants, lawyers, prosecutors, judges as also the law enforcement personnel. Efforts are also being made to provide hi-tech infrastructure; facilities to all those who deal with cybercrime and criminals. Presently, e-judiciary in India is at its formative stage, it will gradually develop as the process of switchover to e-police stations and e-Courts gains momentum in the coming years. However, the problem of extra-territorial jurisdiction of the Courts over perpetrators of cybercrime still remains a grey area because of the variations in criminal law and procedure of different countries. The problem is further complicated because of the anonymity of the
perpetrator of internet crime and his physical non-existence at the scene or place of crime. These issues cannot be resolved by a nation unilaterally unless all the countries involved and affected by the cybercrime join together and extend cooperation in nabbing the criminals and getting them punished.

-------------