Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Cybercrimes: The Judicial Response & It's Perspective

Dr. Bhavish Gupta[1], Dr. Sachin Kumar Goyal[2]

[1]*Professor & HoD-Law, IMS Law College (Affiliated to CCS University, Meerut), Noida*
[2]*Associate Professor, IMS Law College (Affiliated to CCS University, Meerut), Noida*

Cybercrime refers to criminal activities that involve computers, networks, or digital systems, with perpetrators exploiting technology to commit illegal acts. It encompasses a wide range of offenses, including identity theft, financial fraud, hacking, cyberbullying, ransomware attacks, and intellectual property theft. As digital technologies continue to evolve, cybercriminals have become more sophisticated, targeting individuals, corporations, and even government institutions. The anonymity and global reach provided by the internet have made it easier for criminals to perpetrate these crimes, making it challenging for law enforcement agencies to investigate and prosecute offenders effectively. Additionally, it undermines trust in digital platforms, impeding the growth of the digital economy. Lawmakers and cyber security experts continue to develop new strategies to combat cybercrime, including enhanced legal frameworks, international cooperation, and advanced technological solutions like artificial intelligence and block chain. Understanding the nature, impact, and emerging trends in cybercrime is crucial to developing effective prevention and response strategies in our increasingly digital world.
Keywords: Cyber Crime, Cyber bullying, Cybercriminals, Judiciary.

1. Introduction

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 and

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 cyber crime cases are as follows:

(i) Global nature of these crimes is such that they do not recognize 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

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 , 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 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 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 , the case involved an issue where the petitioner, P.R. Transport Agency, was seeking relief in a matter related to an alleged cybercrime incident, where certain illegal activities, including the misuse of digital platforms, were taking place. The case primarily revolved around the applicability of the Information Technology Act, 2000 and how it could be enforced in the context of crimes involving electronic records, digital platforms, and online activities.

The case dealt with the question of intermediary liability and the responsibility of platforms to ensure that their services were not being misused for unlawful purposes, particularly in the context of the dissemination of illegal material or the facilitation of cybercrimes.

The case helped clarify some key aspects of Section 79 of the Information Technology Act, 2000, which provides a "safe harbour" for intermediaries, shielding them from liability if they act as neutral platforms and if they promptly take down illegal content upon receiving notice.

This case is significant in the context of cybercrime law as it provided some legal clarity on the responsibilities of digital service providers, intermediaries, and online platforms in preventing or addressing cybercrimes. It also discussed the limitations and scope of the safe harbor provisions for intermediaries under the IT Act.

While the case is not as widely known as others in cybercrime jurisprudence, it is an important reference in understanding the evolving landscape of intermediary liability in India.

CYBER PORNOGRAPHY: JUDICIALTREND

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 a 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 the mare disposed of in the lower Court at The magisterial level.

However, the case of State of Tamil Nadu v. Suhas Katti , 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 accounting the name of the victim. The e-mails carried a message that the victim Decided by the Chief Metropolitan Magistrate, 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 Section509 of IPC, and a sentence to undergo simple imprisonment of2yearsand 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.

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 within38 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 Rizwana v. State , Fatima Rizwana filed a complaint against an individual who had created a fake social media profile in her name and used it to harass and defame her. The accused posted inappropriate and defamatory content online that tarnished the victim's reputation. The victim sought legal recourse under various provisions of the Indian Penal Code (IPC) and the Information Technology Act, 2000, alleging that the defendant was guilty of cyber stalking, online defamation, and other related offenses.

The key legal issues in the case included:

Section 66C of the Information Technology Act, 2000: For identity theft and fraudulently using someone's identity online.

Section 66D of the Information Technology Act, 2000: For cheating by impersonation using a computer resource.

Section 507 of the IPC: For criminal intimidation by anonymous communication.

Section 500 of the IPC: For defamation.

The case highlighted the legal recourse available to victims of online harassment and the applicability of cyber laws in tackling offenses like defamation, stalking, and harassment committed using digital platforms.

The Delhi High Court in this case ruled in favour of the victim, emphasizing that creating fake profiles and using them for malicious purposes is a serious cyber offense. The accused was charged under relevant provisions of the IT Act and IPC. The court also stressed the importance of protecting individuals' rights and reputations in the digital space.

The Fatima Rizwana v. State case is notable because it underscores the growing importance of legal protections against cyber harassment and online defamation in India. It also helped clarify the application of cyber laws in cases involving identity theft and online impersonation, which have become increasingly prevalent with the rise of social media and digital platforms. The case serves as a reminder of the legal remedies available to victims of cybercrimes.

JUDICIAL CONCERN FOR IPR REALTED CYBER CRIMES

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 43of 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 Diesel Reconstruction (P) Ltd. V. Kirloskar Proprietary Ltd. 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 Section105(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 of the use of that mark. In this case, the Court restrained the defendant from using the trade name' Kirloskar' for the ir 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 Himalaya Drug Co. v. Sumit 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 data base of more than 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. 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.

In yet another case, namely Dalgit Titus, Advocate and others v. Alfred A. Adevare and others 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 retainedcontroloverttheprofessionalorganisation.Theyclaimedcopyrightownershipoverthewor k which they had done while working in the plaintiff's legal firm. The plaintiff's, on the other hand, contended that since the defendant were a part and parcel of the plaintiff's firm, they could not claim exclusive right in respect of data base 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 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 7.2GB of database of their crucial data ,write-up through plaintiffs local area net work 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.

The American case of Marks and Spencer PLC v. One in million , 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 land mark case of American Civil Liberties Union (ACLU) v. Reno , may be followed to arrive at a correct finding. In that case, it was 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 connection. In fact, host actually possesses two addresses i.e. a numerical 'IP' address suchas125, 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 Centre. 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.

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 , 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 ILR 2005 Kant (decided on January 31, 2005). SalesTaxAct,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 2of 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.

JUDICIAL TREND IN OTHER CASES

The Supreme Court in M/s Satyam Infoway Ltd. v. Sifynet Solutions (Pvt.) Ltd 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 , 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 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 20-25dressings 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 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.

2. Conclusion:

The judicial approach to cybercrime has evolved significantly over the past few decades in response to the growing threat of digital offenses. Courts worldwide have made notable strides in interpreting and applying existing laws to address the complexities of cybercrime, though challenges persist due to the rapid pace of technological advancements. The judiciary plays a critical role in shaping legal frameworks that not only deter criminal activities in cyberspace but also ensure justice for victims of online offenses, while safeguarding fundamental rights such as privacy and freedom of expression.

While various legal instruments, such as the Cyber security Act and Computer Fraud and Abuse Act, have provided a foundation for prosecuting cybercriminals, the international nature of cybercrime presents unique difficulties for enforcement. The need for global cooperation, harmonized legal standards, and specialized judicial expertise is more urgent

than ever. Courts must continue to balance the protection of digital infrastructures and privacy with the need to uphold civil liberties in a digital age.

Additionally, the judiciary's role extends beyond mere adjudication. Courts must also promote legal reforms, encourage the development of new technologies to fight cybercrime, and support the creation of specialized units within law enforcement to better combat cyber threats. As cybercrime grows more sophisticated, the judicial approach will need to remain dynamic, adaptable, and proactive in ensuring that justice prevails in the ever-changing digital landscape.

References

Professor & HoD-Law, IMS Law College (Affiliated to CCS University, Meerut), Noida
Associate Professor, IMS Law College (Affiliated to CCS University, Meerut), Noida
AIR2006SC2820 (Para11)
2007 (4) JCC 3157 (Delhi)
(2004) 7 MLJ 60 (Mad)
2005 (2) JCC 770 (Delhi).
2011 (2) JCC 1120 (Delhi)
Intellectual Property Rights are referred to as 'IPR
AIR1996Born.149
2008 (36) PTC 62 (Del)
(2004) 121 DLT 268 (Delhi High Court)
[1998] 4 All ER 30 (Chancery Division, High Court of Justice, UK)
521 U.S. 844 (1997)
2006 (146) STC 641 (Karnataka)
AIR2004SC3540
AIR2003SC 2053