JURISDICTION IN CYBERSPACE

| Authored By : Ms. Toshi Tiwari |

5.1. Introduction

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

There are many issues to be resolved in Cyber law. Two areas of cyber law requiring further clarification are cyber crime and jurisdiction. For example, in cyber law there are only a limited number of cases on point and no major statutory schemes on the books. Policy makers and attorneys dealing with cyber crime are often confined to referring to the imprecisely applicable and scarce existing statutes and cases[28].

In cyber jurisdiction, the Court must address the question of which lawmaker has jurisdiction over actions taking place on the Internet. In the few cases the Courts have adjudicated, they have applied long-arms statutes and personal jurisdictional principles in making decision. Due to the paucity of cyber jurisdiction cases, there is a limited amount of law for the legal practitioner for reference.

5.2. Cyber Threats

The FBI defines a cyber incident as "a past, ongoing, or threatened intrusion, disruption, or other event that impairs or is likely to impair the confidentiality, integrity, or availability of electronic information, information systems, services, or networks" (2017). While data breaches can happen in many ways, this article focuses on the potential for targeted attacks.

Four types of cyberattacks are particularly concerning for state courts.

1. **Phishing** uses social engineering to solicit personal information from unsuspecting users to compromise their own systems. Phishing e-mails appear legitimate and manipulate users to enter items, such as usernames or passwords, that can be used to compromise accounts. Spearphishing, a more personalized method, could target specific judges and court employees.

2. **Ransomware** infects software and locks an organization's access to their data until a ransom is paid. Through phishing e-mails, drive-by downloading, and unpatched software

[28] Stewart Biegel, The Emerging and Specialized Law of the Digital Revolution, Los Angele Daily Journal, Jan. 25, 1996.

vulnerabilities, cybercriminals attempt to extort users by encrypting their data until certain conditions are met. The result is a temporary or even permanent loss of data.

3. **Advanced persistent threat (APT)** attacks attempt to maintain ongoing, extended access to a network by continually rewriting malicious code and using sophisticated evasion techniques. A successful APT attack results in complete invisible control of systems over a lengthy period time. APTs typically use socially engineered attacks to get a foot in the network door.

4. **Code-injection attacks** involve the submission of incorrect code into a vulnerable computer program without detection. Through these attacks, cybercriminals trick the target system into executing a command or allowing access to unauthorized data. The most common code injection attack uses Standard Query Language (SQL) through an online application.

5.3. Cyber security

In our hyper-connected world, the technology that we rely on also makes us more vulnerable. State court systems are no exception. The many benefits of technology are accompanied by risks and challenges. Unfortunately, cyberattacks on individuals and organizations continue to rise in frequency and sophistication. The Federal Bureau of Investigation (2017) reported that cyberattacks in the United States caused over $1.3 billion in victim losses during 2016. Generally, cybersecurity involves the protection of computers and information systems from theft, damage, or disruption. More specifically, Craigen, Diakun-Thibault, and Purse (2014) define cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights"[29]

5.4. Cyber Jurisdiction

The term "jurisdiction" refers to the authority of a court to hear a case to resolve the dispute. In other words, court's power to decide a case or issue a decree depends upon its jurisdiction. Since the legal environment of e-commerce has no geographical boundaries, cyber jurisdiction extends to all communications to anyone who has access to website.[30]

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

The Internet can be seen as multi-jurisdictional because of the ease which a user can access a Web site anywhere in the world. It can even be viewed as a-jurisdictional in the sense that from the user's perspective state and national borders are essentially transparent.[31]

[29] https://www.ncsc.org/~/media/Microsites/Files/Trends%202018/Cybersecurity-Protecting-Court-Data-Assets.ashx

[30] Ferrera G.R.: Cyber Law: Text and Cases (2001, Ohio) p.4.

[31] David Post, Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace, 1995 J. Online L. art.3,Para. 36.

For courts determining jurisdiction, however, this situation is more problematic. The court in Zippo Manufacturing Co. v. Zippo Dot Com Inc.[32] said there is a global revolution looming on the horizon, and the development of the law in dealing with allowable scope of personal jurisdiction based on Internet use is in its infancy.

The developing law of jurisdiction must address whether a particular event in Cyberspace is controlled by the laws of the state of country where the Website is located, by the laws of the state or country where the Internet service provider is located, by the laws of the state or country where the user is located, or perhaps by all of these laws[33].

Cyber jurisdiction issues have been dealt with primarily in the civil courts. Since the advent of U.S. v. Thomas[34], and Minnesota v. Granite Gate Resorts Inc[35]., however, cyber jurisdiction issues have begun to be examined in criminal courts as well.

5.5. Targeting Courts

State court systems are guardians of sensitive data for individuals and organizations. Court records are crucial in the functioning of our society. Preserving these official records is a responsibility long held by judicial-branch administrators. The Judiciary Act of 1789 created the first position of district court clerk to record deeds and judgments of the courts (Sec. 7). Much has changed in the nearly 229 years since. Today, modern court administrators have extensive data-governance responsibility. Data governance includes the people, processes, and technology required to properly handle an organization's data assets. Included under this umbrella are data quality, usability, integrity, security, and preservation. Data governance truly touches all aspects of a court organization.

The landscape of court technology has changed rapidly, as digital tools help facilitate the business process of the court. This proliferation of technology has improved the judiciary's access and transparency, while also significantly increasing data storage and the digital footprint. Consequently, there are multiple entry points for data breaches in the judicial branch. These include judiciary case management systems, networks, servers, cloud storage, software programs, Wi Fi systems, employee devices, and an array of court-specific technology. No longer is just one desktop PC assigned to each employee within a court facility. Judges and court staff now use laptops, tablets, and smart phones to conduct court business. These devices are used outside the confines of the courthouse, accessing networks within and across jurisdictional lines.

5.6. Responding to Cyber attacks

Even with the best of intentions and diligent preventative measures, data breaches happen. A cyber-incident response team should be created in the planning process. Immediate, strategic action on the part of the victimized organization is required to minimize damage and expedite recovery. Essential first steps for courts include pinpointing the area of intrusion, minimizing exposure and attack surface, and understanding the scope of the attack. For example: Was just a family-court case management system compromised? Was the breach confined to only

[32] .USDC, Western District of Pennsylvania, 1997 952 F. Supp. 1119, http://zeus.bna.com/elaw/cases/zippo.html
[33] Stuart Biegel, supra note 9, at 2
[34] 74 F. 3d 701 (6th Cir. 1996) (USA)
[35] 568 N.W. 2d 715 (Minn. App. 1997); aff'd 576N.W.2d 747 (Minn. 1998)

certain courts in the state? Data on all attack-related events must be collected and logged, as it will be vital in the attack investigation. After a breach is discovered, the attack should be reported to at least one law-enforcement agency. Within the federal executive branch, the United States Department of Justice, Department of Homeland Security (DHS), and FBI provide guidelines and best practices for responding to cyber attack incidents. These agencies supply secure forms to report cyber incidents for analysis. The Multi-State Information Sharing and Analysis Center (MS-ISAC), created by DHS, is the key resource for cyber-threat prevention, protection, response, and recovery for state and local governments. MS-ISAC is a voluntary and collaborative effort that serves as a central resource for situational awareness and incident response for state and local governments. Membership is open to all state and local governments at no cost. The Washington State AOC collaborated with MS-ISAC to determine the scope of their 2013 data breach. In addition to data-asset threats, shutting down court systems because of a cyber attack can have massive operational impact on normal court business. In these instances, courts must be able to hold time-sensitive and constitutionally mandated hearings, as well as issue warrants and orders. Courts also have to consider filing access for those parties bound by a filing statute of limitations. When necessary, impacted jurisdictions can issue an order tolling case activity during operational disruption. Sharing timely and accurate information to all impacted by the breach is crucial. Once the type of attack is identified and understood, sharing this information with other court systems is beneficial. Creating a heightened awareness for specific attacks, along with actionable information, provides great value to the court community.

1. Cyber Jurisdiction In Civil Cases

In determining whether jurisdiction exists over a defendant, the U.S. Federal courts apply the law of the forum state, subject to the limits of the Due Process Clause of the Fourteenth Amendment.[36]

In Inset Systems, Inc. v. Instruction Set, Inc.[37] the court held that advertising over the internet was purposefully directed toward the forum state.

The US District Court for the Eastern District of Missouri reached a similar conclusion in Martiz, Inc. v. Cyber Gold, Inc.[38] finding that it had jurisdiction over a California defendant in a trademark infringement case, where the defendant‘s only contact with the state was through its California based website, which was accessible in Missouri.

In McDonough v. Fallon McElligott, [39]the court dismissed plaintiff‘s contention stating that ―because the web enables easy worldwide access, allowing computer interaction via the web to supply sufficient contact to establish jurisdiction would eviscerate the personal jurisdiction requirement as it exists. Thus, the fact that defendant has a web site used by Californians cannot establish jurisdiction by itself[40].

[36] U.S.C. Const. Amendment. XIV
[37] 937 F. Supp. 161 (D. Conn. 1996)
[38] No. 96-CV01340 (E.D. Mo. Aug. 19, 1996)
[39] No. 95 Cir 4037 (S.D. Ca. August 15, 1996)
[40] Supra note 14

Similar decision is Pres-Kap, Inc v. System one, Direct Access, Inc.[41] which involved electronic contacts through a computerized airline reservation system. In Burger King Corp. v. Rudezuitiz[42] the US Supreme Court asserted jurisdiction on the grounds of accessibility of Internet. The court asserted that when a defendant has purposefully directed its activities to a forum state and caused injury to an individual or entity, the state's invocation of jurisdiction comports with its Due Process obligations[43].

2. **Cyber Jurisdiction In Criminal Cases**

The question of cyber jurisdiction in a criminal case came to the forefront of attention in early 1996 in U.S. v. Thomas[44] when the Sixth Circuit upheld the highly publicized conviction of a couple operating a pornographic bulletin board from their home. The defendants began operating the Amateur Action Computer Bulletin Board System (AABBS) from their home in Milpitas, California in February 1991. The AABBS contained approximately 14,000 Graphic Interchange Format (GIF) files. These files could be accessed by members who possessed the password. Once the password was entered, the users were able to select, retrieve, or download the GIF files to their own computers.

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

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

The defendant asserted that the GIF files were an intangible string of 0's and 1's, which only became viewable images after being decoded in the AABBS member's computer. The court disagreed, ruling that the fashion in which the images were transmitted did not affect their ability to be viewed or printed out by members in Tennessee. The defendant also argued that they were prosecuted under the wrong statute and that their conduct, if criminal at all, fell within the prohibitions of the statute which addresses commercial dial-a-porn operations[45] The court declined to accept this argument. Instead, it ruled that the statute must be construed to affect the intent of Congress, which was to prevent the channels of interstate commerce from being used to disseminate any obscene matter.

[41] 636 So. 2d 1351 (Fla. Dist. Ct. App. 1994)
[42] 471US 462 (1985)
[43] Steven Jensen, ―Jurisdiction of the Internet: The Courts and Alternatives Solutions‖, at http://www.suffolk.edu/law/hightech/classes/cyberlaw/siensen/ppaper.html
[44] 74 F.3d 701 (6th Cir. 1996)

[45] U.S.C. section 223(b) (1934, amended 1988).

3. Cyber Jurisdiction In International Cases

When adjudicating cases involving foreign nationals, the courts must balance several factors. On a case-by-case basis, the courts must consider the procedural and substantive policies of other countries whose interests are affected by the court‘s assertion of jurisdiction. Keeping these policies in mind, the court must then consider the reasonableness of assertion of jurisdiction examined in the light of the interest of the federal government in its foreign relation policies. When extending jurisdiction into the international field great care and reserve must be exercised[46].

Because of these sovereignty concerns, there is a higher jurisdictional barrier when litigating against The Supreme Court in Asahi Metal Industry Company v. Superior Court,[47] indicates that a plaintiff seeking to hale a foreign citizen into court in the United States must meet a higher jurisdictional threshold than is required when the defendant is a United States‘ citizen. In Asahi the court found that even though Asahi had minimum contacts with the forum state, it would be unreasonable and unfair to find jurisdiction for three reasons: (1) the distance between defendant‘s headquarters in Japan and the Superior Court of California and the unique burdens of submitting a dispute between two foreign nationals in a foreign legal system; (2) California‘s and the foreign plaintiff‘s slight interest in having the case heard in California; (3) the affect on the procedural and substantive interests of other nations by California‘s assertion of jurisdiction over a foreign nationals.

4. Cyber Jurisdiction In Information Technology Act, 2000

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

The Information Technology Act, 2000 specifically provides that unless otherwise provided in the Act, the Act also applies to any offence or contravention there under committed outside India by any person irrespective of his nationality[48] . It is however clarified that the Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention, involves a computer, computer system or computer network, located in India.[49]

The words ‘act’ or ‘conduct’ constituting the offence or contravention involves a computer, computer system or computer network located in India are very significant to determine jurisdiction of the IT Act over acts committed outside India. For assuming jurisdiction over an act constituting an offence or contravention under the IT Act, which is committed outside India, it has to be proved that the said act involves a computer, computer system or computer network located in India.

[46] Asahi Metal Industry Company v. Superior Court, 480 U.S. 102 (1987)
[47] 480 U.S. 102 (1987).
[48] Sec. 1(2) of IT Act, 2000
[49] Sec. 75 of IT Act, 2000

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

Another instance to explain the jurisdiction of the IT Act is where a person from the US hacks a computer system or network in India, section 66 of the IT Act would come into play to punish the accused for hacking because his act involves a computer in India. Similarly, where a person anywhere in the world plants a virus into a computer system located in India, he would be liable under Section 43(c) of the IT Act to pay damages by way of compensation net exceeding Rs. 1 crore to the victim.

Section 75 of the IT Act is restricted only to those offences or contraventions provided therein and not to other offences under other laws such as the Indian Penal Code, 1860. Jurisdiction over other cyber crimes, for instance under the Indian Penal Code, 1860, has to be determined by the provisions of the Criminal Procedure Code, 1973. The fundamental principle on jurisdiction is the same under the IT Act[50] and the Criminal Procedure Code, 1973, though stated differently. The basic legal principle of jurisdiction under the Code of Criminal Procedure, 1973 is that every offence shall ordinarily be inquired into and tried by a court within whose local jurisdiction it was committed.[51]

In a case where an act is an offence by reason of anything, which has been done and of a consequence, which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such act has been done or such consequence has ensued.[52] For instance, in a case of defamation, either of the courts, i.e. of the place from where the defamatory letter was e-mailed and the place at which it was published or received, if different, shall have jurisdiction to inquire and try the same.

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

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

The law of jurisdiction stated in the Criminal Procedure Code, 1973 and Section 75 of the IT Act, 2000, as discussed herein, is clear, specific and covers different situations which are likely

[50] Sec. 1(2) r/w Sec. 75 of IT Act, 2000
[51] Sec. 177 of Cr. P.C., 1973
[52] Sec. 179 of Cr. P.C., 1973

to generally arise in cyber crime cases. The internet by its nature and purpose operates when the parties interacting or transacting are not physically face to face with one another.

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

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

5.7. Judicial Trends in India

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

- **Judicial Response on Online Fraud**

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

- **Judicial Response on Credit Card Fraud**

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

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

- **Judicial Response on Defamation**

Every person has a right to have his reputation preserved inviolate. This right of reputation is acknowledged as an inherent personal right or every person. It is a jus in rem, a right good

against the entire world. A man's reputation is his property, more valuable than other property.[53]

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

- **Judicial Response in Protection of Intellectual Property Rights**

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

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

- **Judicial Response on Copyright Violation**

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

In Lotus Development Corporation v. Pareerback Software International[54] it was held that commuter programs like any other works are copyrightable.

- **Judicial Response on Cyber Squatting**

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

[53] Dixon v. Holden, (1869) LR 7 Eq 488
[54] (1990) 240 F. Supp. 37 (US)

bad faith internet to profit from the goodwill of a trademark belonging to someone else. The cyber squatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price[55]

- **Judicial Response on Phishing:**

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

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

- **Judicial Response on Online Gambling**

Gambling in India is prohibited under the Public Gambling Act 1867. However the word _gambling' is not defined in the Public Gambling Act 1867. According to the Supreme Court of India, ―Gaming is the act or practice of gambling on a game of chance. It is staking on chance where chance is the controlling factor. Internet gambling is traditional crime of gambling where computer is used as tool provided it is otherwise is an offence in a particular jurisdiction.[56]

There are thousands of Websites that offer online Gambling. The special issue with online gambling is that it is legalised in several countries. So legally the owners of these websites are safe in their home countries. Virtual casinos, Cases of money laundering etc are online cases.[57]

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

- **Judicial Response on Cyber stalking**

Stalking in common parlance means a harassing or threatening behavior which an individual exhibits towards the other. If an individual uses cyberspace for stalking then it is called cyber stalking. Thus, cyber stalking is an online course of conduct of a person by which the targeted person is terrorized, embarrassed, ashamed, molested, outraged, or frightened.

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

[55] Karnika Seth: Cyber Laws in the Information Technology Age, Edn. Ist 2009, Lexis Nexis Butterworths Wadhwa Nagpur, p- 452
[56] Balwinder Kaur: Internet Gambling, Criminal law Journal, October 2008- Journal Section
[57] Prashant Mali: Cyber Law & Cyber Crimes, Ist Edn. 2012, Snow White Publications. P-82

globe, but he can now impersonate the victim to harass or humiliate him. It is now not necessary for stalker to disclose his identity.

- **Judicial Recognition to Electronic Documents**

Consequent to passing of the Information Technology Act, 2000, electronic documents have come to be recognized at par with the written documents for the purpose of evidence in law. Similarly, the digital signatures[58]affixed in accordance with the provision of Section 5 of the IT Act, 2000, will be considered equivalent to written signatures. All electronic documents either in the electronic form itself or as certified print-out thereof shall be admissible under the Indian Evidence Act 1872. The recognition of electronic document as a valid evidence admissible under the law of evidence has been facilitated the prosecution of cyber criminals and establishing their guilt on the basis of such evidence.

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

- **Judicial Response on Hacking (Unauthorised Access)**

Hacking means unauthorised access to computers. When a person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means with intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, he is said to have committed an offence of hacking.[59] The person who commits an offence of hacking is called hacker. Webster's Dictionary defines the term 'hacker' as a computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance[60]

- **Judicial Response on E-Mail Misuse**

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

- **Judicial Response on Illegal Online Selling**

It is becoming increasingly common to find cases where sale of illegal articles such as counterfeit currency, counterfeit branded products, narcotics drugs, weapons, wildlife etc. is

[58] The expression _Digital Signature' has been replaced by the term _Electronic Signature' by the I.T. (Amendment) Act, 2008.
[59] Section 66 of the IT Act, 2000
[60] Webster's new World Dictionary of Computer Network Abuse, 6 Harv. J.L. & Tech.307, 310 n. 7 (1993).

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

5.8. Conclusion

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

There has been significant change in the judicial trend with regard to adjudication of cybercrime during the past two decades. Realising the fact that data stored, processed and transmitted in the electronic form is not directly tangible; the courts while adjudicating on cyber cases no longer adhere to strictly rigid and literal interpretation of law but adopt a more pragmatic and practical approach to the problems involved in the case before them for disposal, without, however, deviating from the basic intent of the legislature in enacting the law applicable to the case.

In view of the expanding dimensions of cybercrimes in India in recent years, it is not only the police force but also the judicial officers at the lower as well as higher level, who need to be properly educated and trained in various technological aspects of cybercrimes. In the present scenario, the perpetrators of these crimes are moving much faster than the law enforcement agencies in exercising effective control over them. The need of the time therefore, is that the judiciary should move faster than the law enforcement agencies in excersing effective control over them. The need of the time therefore, is that the judiciary should move faster than the cyber criminals by expediting disposal of cyber cases within a time-frame and make sure that the guilty do not escape punishment due to vagaries of law and evidence. As it has been rightly said, the threat at present is not from the intelligence of the cyber criminals but it is from the ignorance and lack of will to fight against cyber criminality‖. It may be reiterated that computer is a tool as well as a target for the preparation of cybercrime. The Information technology Act, 2000 specifies the illegal acts which have been made punishable as offences under the Act. The amendments made in the Indian Penal Code, law of Evidence and Criminal Procedure, Banker‘s Book Act and the Negotiable Instruments Act also enable the law enforcement agencies and the judiciary to nab cyber criminals promptly and punish them.

The statistical data of cybercrime in India indicates that the incidents of these crime is constantly on an increase as compared to the rate of conviction which is significantly low the reason being that there is general lack of awareness about the computer crimes among the people who at times even do not know that they have fallen a victim to the illegal activities of perpetrators of cybercrime. In result, most of the crime remain unreported, and a few which are

reported, result in acquittal due to ignorance of the police and investigating officials about the technicalities of these crimes and lack of sufficient evidence against the accused.

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

One of the cyber law experts and Supreme Court lawyer Mr. Pavan 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 practicing in Mumbai has underlined the need for computer friendly lawyers and Judges who are well versed with the functioning of the computer system and its operational pitfalls to handle cybercrime cases.