VOLUME 18 ISSN 2456-9704

ROLE OF JUDICIARY IN CYBER CRIME

By Mehak Aneja
From School of law, The Northcap University

ABSTRACT

Judiciary plays an important role and also wing of the government in resolving the conflicts among the parties in cybercrime. Before going into this research paper, lets know what is cyber- crime. Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

In this research paper we will be discussing about how judiciary played role in cyber crime cases. So many amendments were made in other Acts and also there are many landmark judgments to know how judiciary played role in solving disputes related to cyber crime of different type.

INTRODUCTION

In India the use of internet is growing rapidly. Internet has given rise to new opportunity in every field like education, business, entertainment. Cybercrime is emerging as a serious threat all over the world. Now, government police departments and intelligence units have also started reacting and taking initiatives to reduce these cyber threats. Special cyber cells are initiated by India police.

India judiciary is also very successful in reducing cyber offences by implementation of the provisions of Information Technology Act 2000. These offences are also known as modern day offences which involves computer as a tool or target. The trails are conducted in the court and punishment is given to the accused. To provide punishment to accused. To provide punishment to accused. To provide punishment to accused Information Technology Act is read with criminals laws.

Cybercrime law identifies standards of acceptable behaviour for information and communication technology users. It also establishes socio-legal sanctions for cybercrime; mitigates and prevent harm to people, data, services, systems, infrastructure in particular; protects human rights; and also enables prosecution and investigation of crimes which are committed online. They also facilitate cooperation between countries on cybercrime matter. There are some cybercrime laws which provides standards of behaviour and rules of conduct for the use of the internet, computers and related digital technologies.

On the 14th august 1995, the 48th anniversary of Indian independence, India launched a full internet service for public access. In 1998, just after the few years VSNL introduced dial-up internet and around 0.5% of India's population has regular internet access. By 2013, 15% of the countries were connected with the internet and the number is growing exponentially. As the influence of the internet grew the law and the courts began to take notice.

INFORMATION TECHNOLOGY ACT, 2000

International trade through electronic means was spreading in many countries and has turned over from paper base commerce to E-commerce. With this globalization of trade and business, the international community felt a need of such law which would set uniform standards for electronic commerce. This thought led to adoption of model law on electronic commerce by UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL).

First, legislation was passed by Indian parliament in the 51th year of the Republic of India called as Information technology Act, 2000. India enacted the Information Technology Act, 2000 for providing legal recognition to the transaction which are carried out by means of electronic data interchange or electronic communication and also to facilitate electronic filings of documents with the government agencies. Due to this some Acts were amended
Indian penal code, 1860[1]
Indian evidence Act, 1872[2]
Bankers books evidence Act,1890
Reserve bank of India Act, 1934
Though since 2000 the IT Act was in place in India for curbing cybercrime, but the problem was still that these statutes were only on paper than on execution because layers, police officers, prosecutors and judges feel handicapped in understanding its highly technical terminology.

CYBER CRIME UNDER INFORMATION TECHNOLOGY ACT, 2000

This Act deals with cybercrimes. The provisions relating to cybercrime are given under chapter XI of IT Act, 2000 under the heading of 'offences' which deals with various types of offences which are done through electronic form like computer, computer system, computer networks.
Cybercrime and cyber offences are never defined under IT Act, 2000. Various legislative provisions with respect to various cyber crimes in India are given as follow: -

1. Tampering with computer source document
2. Computer related offences
3. Sending offensive messages through communication services etc.
4. Identify theft
5. Violation of privacy
6. Cyber terrorism
7. Publishing or transmitting obscene material in electronic form (cyber pornography)
8. Breach of confidentiality and privacy
9. Offences related to electronic signature certificate
10. Offences by companies.

JUDICIAL RESPONSE

Cybercrime is of intangible nature; it does not require any physical presence or physical violence at the scene of crime. Under these circumstances, the adversarial system of litigation would hardly meet the ends of justice in cases relating to cybercrime. the problem faced by the judiciary and the enforcement agencies in dealing with computer related crimes, the Supreme Court of India in **State of Punjab and Others v. M/S Amritsar Beverages Ltd. and Others** observed that:

[1] SECTION 9, 192, 464, 466, 468, 469, 471, 474, 476, 477A of Indian penal code, 1860

[2] SECTION 47A, 65B, 67A, 73A,81A,85A,85B,85C,88A,90A OF Indian evidence Act,1872

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

Indian judiciary has played on important role in handling cybercrime cases in cyber age because the Supreme court of India is the ultimate interpreter of laws over the decades. The judicial and law enforcement agencies only well understand that the means available to investigation and prosecute crime and terrorists act which is done through the medium of computer are present almost wholly and national in scope. But still the Indian judiciary improved and come up with the amendment of laws and also handled so many cases related to different types of cybercrimes. Some of the important judgements given as follow:

1. **Tampering with computer source document:**

Tampering means to interfere with something in order to cause damage or make authorized alterations. The Indian judiciary is playing important role in dealing with offences relating to the tampering with computer source document.

Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr

This is the first case which is related to IT Act Sec 65[3] In this case the court held that the cell phones fulfilled the definition of computer under IT Act and the unique electronic serial numbers which are programmed into each handset like SID(system identification code), MIN(mobile identification number), are the computer source code under the definition of IT Act which is required to be kept and nominated by law.

In Sanjay Kumar v. State of Haryana

The petitioner has been convicted for an offence punishable under section 65 and 66 of IT Act read with 420, 467, 468 and 471 of IPC and sentenced for rigorous imprisonment but the petitioner filed an appeal against such order which was dismissed by the appellate court and upheld the trial court judgment. In this case the manager of Vijay Bank, NIT, Faridabad, filed a complaint to police by stating that the petitioner was deputed by M/S Virmati Software and Telecommunication Ltd. to maintain the software system supplied by them to the Bank. But the petitioner has manipulated the interest entries of computerized bank account and thereby cheated the complainant bank by forging electronic record in order to cause wrongful loss to the bank.

2. **Computer related Offences:**

[3] Tampering with computer source documents.- Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Indian judiciary has played a vital role in dealing with cases related to computer offences which falls under cybercrime.

In Kumar v. Whiteley

The accused gained the unauthorized access to the Joint Academic Network and deleted, added files and changed the passwords to deny access to the authorized users.

It was revealed by the investigations that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and made alteration in the computer database pertaining to broadband Internet user accounts of subscribers. The Additional Chief Metropolitan Magistrate, Egmore, Chennai sentenced him to undergo a rigorous imprisonment for one year with a fine under section 420 of Indian Penal Code[4] for cheating and section 66 of Information Technology Act[5] for computer related offence through communication service, etc.

In State of A.P v. Prabhakar Sampath

The complainant M/S SIS Infotech Pvt. Ltd., Hyderabad, carrying the business of research station, filed a complaint by stating that somebody successfully hacked their server and downloaded their e-reports through some free public sites. After investigation made by the police, the accused was found guilty and charged under section 66 of IT Act for hacking content server of complainant's company.

3. **Sending offensive messages through communication services etc:**

Judiciary played a well role in solving cases related to sending offensive message. The Additional District Court and Sessions Court was upheld a lower court's verdict in the first cyber case in **State v. Ts. Balan and Aneesh Balan** (2006) and sentenced a Pentecostal priest and his son for morphed photographs and e-mailed to victims from fake IDs with captions under section 67 of Information Technology Act, 2000.[6]

In *Shreya Singhal v UOI*, (2013) 12 S.C.C. 73(interim relief)

A public interest litigation was filed before the Apex court challenging constitutionality

[4] Cheating and dishonestly inducing delivery of property.—Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

[5] Computer related offences. -If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. Explanation. -For the purposes of this section,-
(a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);
(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).]

[6] Punishment for publishing or transmitting obscene material in electronic form. -Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

of Section 66A of the IT Act,2000[7] wherein State of Maharashtra was called upon to explain the manner of the arrest of two Muslim girls for writing posts on Facebook relating to closure of Mumbai over Bal Thackeray's death. Later, Ministry of Information Technology also issued an advisory on implementation of Section 66A dated 9 Jan 2013 that requires police not to arrest any person under Section 66A till approval is taken from Inspector -General of Police or Superintendent of Police at district level.

The Hon' SC declared section 66A as unconstitutional in its entirety and against the freedom of speech and expression and struck it down in Shreya Singhal and others' v. Union of India. This section had been misused by police in various states to arrest the innocent person for posting critical comments about social and political issues on networking sites. This section had led to the arrest of many people's for posting content deemed to be allegedly objectionable on the internet.

4. Identity Theft:

Role of judiciary in dealing with cyber crime related to identity theft.

Vinod Kaushik and ors. V. Madhvika Joshi and ors

In this case the issue was raised that whether the wife accessed husband's and father-in-law email account without their permission to acquire evidence of dowry harassment. In this case court held the wife liable under section 66C of IT Act, 2000 [8]for unauthorised access and dishonest use of password of any person.

5. Violation of privacy:

Judiciary played in dealing with cases on violation of privacy. Section 66E of IT Act,2000 provides punishment to those persons who intentionally on knowingly capture, publishes or transmits the image of private area of the person without consent. Any electronic transfer of the image through emails, internet, message, Bluetooth is an offence. It doesn't matter whom it is send read it or not but it leads to violation of privacy.

Motion v. state

Sting operation made by a private person or an agency, which may result in violating bodily privacy of another person will fall under sec 66E and shall be liable under the IT Act,2000.

On Feb. 17, 2017, a 24-year-old cybercrime accused and his two aides who are wanted in cybercrime cases, walked into the cybercrime police station, Mumbai, posing as vigilance

[7] Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,—

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

[8] Punishment for identity theft. -Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

officers and tried to conduct a sting operation on the investigation officer. They wanted to blackmail the senior police inspector of the cybercrime cell to not take any action against the accused. However, their spy pen camera did them in. Subsequently, the police found that the three men had fake Central Vigilance Commission (CVC) identity cards and fake letterheads with the names of CBI officers. The Spy camera has been seized. Then the police charged him under section 34 (common intention), 170 (personating a public servant), 174, 419(cheating by personation), 420 and 506 of IPC.

6. Cyber terrorism:

It is a terror or threat against common people or government which is not predictable. Sec 66F defines the punishment for cyber terrorism under IT Act,2000. Terrorist means a person who involves in disruption of services, means communication which is essential for community or indulges in wanton killing of persons or in violence. It also includes hacking, cryptography, trojan attacks and viruses etc.

In 2008 blast in Ahmedabad, Delhi, Jaipur and Bangalore are live examples of cyber terrorism in India. In 2008 attack on Mumbai Taj hotel and again in 2010 the web side of central bureau of identification was hacked by programmers identifying themselves as Pakistani cyber army.

7. Publishing or transmitting obscene material in electronic form (cyber pornography):

Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.

In Sukanto v. State of West Bengalcase which is relating to a magazine 'Nara Nari' as a obscene publication, the under section 292 of IPC convicted the petitioner for giving effect to public morality above art, literature. Indian court followed the principle of obscenity in **Ranjit D. Udeshi v. State of Maharastra** case as given by the U.S. court in **Regina v. Hicklin** case and the honourable court interpreted the word "obscene" and stated that obscene may be defined as "offensive to modesty or decency, lewd, filthy and repulsive". The court also held in the case that it constituted the reasonable restriction on the right of freedom of speech and expression guaranteed under article 19, clause 2 of the Indian Constitution[9] in the interest of decency or morality.

8. Breach of confidentiality and privacy:

The Indian judiciary is playing the important role in dealing with the cyber crimes relating to Breach of Confidentiality and Privacy.

Sharda v. Dharmpal

The Hon'ble Supreme Court held that the right to privacy under article 21 of India Constitution is not an absolute right. If any dispute rose between fundamental rights of

[9] Nothing in sub clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.

two parties then that right would prevail which advances public morality.

Ram Jethmalani v. Union of India

The Hon'ble Supreme Court has dealt with the right to privacy and elaborately held that right to privacy is the integral part of right to life and this has a cherished Constitutional value. Here, it is important to note that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner.

9. Offence related to electronic signature certificate:

The Indian judiciary is playing the important role in dealing with the cyber crimes relating to electronic signature certificate. The Supreme Court defined the term 'publication' in the case of **Bennett Coleman & Co. v. Union of India.** The term 'publication' means dissemination and circulation. The term includes dissemination, storage and transmission of information or data in electronic form if we talk about in the context of digital medium.

10. Offences by companies:

The Indian judiciary is playing the important role in dealing with the cyber crimes relating to offences committed by companies. In the case of **Sheoratan Agarwal v. State of Madhya Pradesh**, it was held that "there is no statutory compulsion that the person-in-charge or an officer of the company may not be prosecuted unless he is ranged alongside the company. Each or any of them may be separately prosecuted or along with the company if there is a contravention….by the company." But this position was overruled in a combined decision by the Supreme Court in the cases of **Aneeta Hada v. M/S Godfather Travels and Tours Pvt. Ltd.** and **Avinash Bajaj v. State** which laid down that prosecution of the company was a condition precedent for the prosecution of the persons who was in charge of or responsible to the company and the director or managing director.

CONCLUSION:

The Indian judiciary has played very successful role in reducing g cyber crime offences under IT Act,2000. Cyber offences are also known as modern day offences. Many amendments were made under different Acts like Indian penal code, Evidence Act to come up with cyber law cases. so from above judgements and from this research paper it is clear that the laws for cyber crime are read with criminal laws to punish the accused.

So, therefore it is concluded that the judiciary or government is very active in identifying cyber-crime and solving it.

REFRENCES

1. Law on cybercrimes : P.K.Singh
2. Justice Yatinder Singh
3. Cyber Law Karnika Seth
4. http://www.researchgate.net
5. www.legalserviceindia.com
6. Shodhganga.inflibnet.ac.in
7.Information Technology Act,2000

*****