International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Cyber Crime in India: A Study on Effectiveness of Cyber Laws in Deterring and Punishing Offenders

Revant Kumar Singh

Student
Email: *rockandrollrevant[at]gmail.com*

Abstract: ***Today we are living in the era of technology where most things are done by computers. With the emergence of technology especially in the field of Artificial Intelligence (AI), we are more likely to depend upon computers. With that increase in dependency, will also increase the chances of crime committed using technology. The crime committed through technology is termed as Cyber-Crime and if there is a crime then there must be a law which is known as Cyber Law. It contains various provisions relating to cyber-crime and their punishments. India has faced many such types of cyber-attacks in the past and still facing them in present. There is always some negative & positive aspect of something whether it's a human or a materialistic object. Technology and Computers too have pros & cons as it has been well said that if technology comes into the hands of bad people, then it might have a detrimental effect on society as well as on mankind.***

Keywords: Cybercrime, Cyberspace, Cyber Law, Information Technology Act, Unauthorized access, Cyber-attack, Dark Web

1. Research Methodology

The methods used in this paper are documentary and doctrinal methods of research. The crucial information was gathered from various articles, existing research papers, books, statutes etc. However, most of the information was gathered from the internet.

2. Review of Literature

There are various existing literature works on this topic which are published by various authors in India, landmark cases cited in Indian Journals and articles published on various websites.

3. Introduction

India has been growing rapidly in the last few decades. As globalization and computerization emerged, the use of computers and technologies also drastically increased. Today almost everyone has access to phones and computers connected through the internet and the use of the same is also increasing day by day. The use of the internet has also resulted in the introduction of a new type of crime i.e., Cybercrime. Criminals committing Cybercrime not only cause notable damages to individuals or the government but also to society and the upcoming generation. The territorial extent of this crime is around the whole globe as there is hardly any country that is secure from the reach of cyber criminals. To regulate and prevent such criminal activities in India, there arises the need to have a Cyber Law which is known as The Information Technology Act of 2000.

4. Cyber Security and Cyber Law

Every person wants physical as well as social security in order to live a healthy life, in the same way, a person using a computer system and surfing the internet also needs virtual protection for privacy and immunities from cyber threats. Cyber security can be defined as the process of protecting computer systems and network systems. It also involves the protection of computer programs, electronic devices, data and identity theft of an individual.

Cyber Law also called as IT (Information Technology) Law is a set of rules and provisions which are made to regulate the activities of an individual or organization in cyberspace.

Areas of Cyber Law

The crucial areas of cyber law include the following:

1) **Intellectual Property**: Cyberlaw covers the intellectual aspect of property. It includes copyright infringement protections.
2) **Scam and Fraud**: Cyber law also covers the prosecution of cyber fraudsters who scam people to obtain financial benefits.
3) **Data Protection**: People are fully dependent on cyber law for the protection of their personal information. Also, the companies are also dependable on cyber law for the confidentiality of their customers.
4) **Harassment**: Online Harassment is one of the Cybercrimes which is a violation of both criminal laws as well as civil. In cyber laws, there are some provisions that deal with this type of crime.
5) **Trade Secret:** Trade secrets are the crucial information of companies commencing businesses. The leakage of the same will cause a great loss to the company. So, to protect against the leakage of trade secrets, cyber law comes into play and restrains the offender from leaking information for monetary gains.

Categories of Cybercrime

In general, there are three utmost categories of Cybercrime:

1) **Cybercrime against Person**: This type of cybercrime occurs on an online platform and affects an individual's daily life. Some of these crimes include identity theft, child Pornography, Defamation, fraud etc.
2) **Cybercrime against Property**: This crime is committed against property such as network systems and electronic devices. Here property includes both tangible and intangible properties. E.g., Copyright infringement and other intellectual property violations are also considered crimes against property.

3) **Cybercrime against Government**: When a Cybercrime is committed against the government of a particular state then it is said to be a Cybercrime against the government. It includes cyber terrorism, hacking government resources and systems, cyber warfare, and stealing crucial data that might compromise the national security of that particular state.

Stages of Cyber-Crime

The crime mentioned in the penal code involves mainly four stages of crime i.e. Intention, Preparation, Attempt & Commission of Crime. According to several researchers, the commission of cyber-crime involves the following stages:

1) **Planning/Preparation**
   Planning is the most crucial stage of a crime whether being a conventional crime or cyber-crime. In this stage, the criminal plans for the execution by preparing methods or making ways to commit a crime by collecting critical information & data, the location of the server etc. Also collects the information related to the security system for the purpose of breaching the same.
2) **Implementation/Execution**
   It includes gaining access to unauthorized systems for the purpose of stealing crucial information, tampering with data, modifying existing stored information etc. with malafide intentions.
3) **Concealment**
   The literal meaning of 'Concealment' is 'to hide'. So, after the commission of cybercrime, the criminal tries to hide his identity as well as the crime by representing it as an error or fault in the system.
4) **Conversion**
   The data or information stolen by the criminals is not kept for a longer duration with them. They immediately convert it into another form by selling the data for financial gains.

Types of Cybercrime

- **Cyber Bullying**: Cyberbullying is a type of cyber-crime in which a person bullies or harasses another person by using electronic devices including social media. It involves the use of messaging applications, social media and even gaming platforms.
- **Phishing**: It is a type of cybercrime which is done through mails. A mail which appears to be from a genuine source is sent to the target which contains a malevolent content and after opening the attachment, it targets personal details such as CVV number, card number and other sensitive information. It is a kind of online fraud.
- **Cyber Defamation**: This type of crime occurs basically through computers and electronic devices. E.g., A person publishing a defamatory content about some other person in messaging group, friends etc.
- **Child Pornography**: This is one of the most serious crime where the offender uses internet to sexually abuse children and circulate the content relating to it.
- **Cyber threatening**: It involves sending of threatening messages and emails to the targeted person for anything which the offender wants to be done by the victim.
- **Email Bombing**: This offense is committed by sending huge number of mails to an individual or a company in order to crash the system or cause a network failure.
- **Hacking**: In order to commit this crime, one must have unauthorized access to a computer system which belongs to other person for the purpose of stealing data and modifying existing information. It is of two types i.e., Ethical Hacking and Unethical Hacking where former is done with bonafide intention and latter with malafide intention.
- **Spamming:** It occurs when an individual receives a huge number of commercial emails and messages which forces them to buy a product or trick them for providing sensitive information like bank account details, card number etc.
- **Denial of Service (DoS) Attack:** It is a type of cyber-attack in which the offender blocks the authorised user or the owner of a computer system from accessing the system, using network system and computer resources.
- **Cyber Terrorism:** It is a new type of terrorism which has emerged in the digital era. It is done carrying terrorist activities using technology and through computer system. This is one of the dangerous cybercrimes which is affecting the whole world. Every terrorist activities happening on this globe has some connection with the cyberspace.
- **SIM Swapping:** In this type of crime, the criminal uses legit information of the victim in order to get access to a new sim card in the name of the victim and use the same for obtaining OTPs and other crucial details over phone.
- **Salami Attack:** It is a type of cybercrime in which the offender tries to steal money from the account of an individual not in lump sum but in small transactions which can't be traced with ordinary examination.

Dark Web

- The Dark web contains all the information other than the information which is available in surface web. In other words, we can say that dark web is like a black hole for which there is no limit as to the content. It can be accessed through only specialized person or browser.
- It is believed that it contains all the critical information and data which can be more than enough to create destruction in the real world. Its content includes weapon purchasing, drugs, contract killing, etc. and other illegal activities. Most of the terrorist attacks are planned and executed with the help of dark web. The sites available on dark web is not indexed anywhere on the surface web or open web and even search engines like Google cannot track these sites.

Preventive Measures

In order to be secured in cyberspace, one must have to take various preventive measures against the threat of Cybercrime:

1) **Create strong password**: a password must be a combination of various letters, numbers and special characters. Also, one must not note it down anywhere in the real world rather he/she must keep it in mind.
   - **Two-step authentication**: This is a new step for securing an account online. In this, a service provider sends a text message over the phone number of the individual which contains a temporary passcode which is put while accessing the account. This provides another security layer so that if a person got your login credentials, then also, he cannot access the account.

2) **Keeping social profiles private**: Social media such as Facebook and Instagram are used for creating a virtual identity of a person by creating a profile on the social networking sites. One must ensure that the profiles remain private so that no one can steal or check the information of others without their permission.
3) **Safeguarding devices**: whether it is a computer or mobile device, one must ensure security against cyber threats by installing various antivirus and total security. Also one must have a strong passcode in the device so that in case of lost or being stolen, the information remains secure.
4) **Visiting unsafe websites**: One must ensure not to visit any unsafe website which could harm the system. Also, one must not click any pop-up on a website because it might install unwanted application which may contain malwares.

Case History

1) AIIMS Cyber Attack, 2022
The All-India Institute of Medical Sciences, Delhi faced an attack on its server in November, 2022. The attack took place due to improper network segmentation and it was estimated that 1.3 terabytes of data was stolen along with the details of 3-4 crore patients including details of high-profile politicians. A case of extortion and cyber terrorism was registered and it was found that the hackers were from China.

2) Cyber-attack on Cosmos Bank
In the year 2018, a bank in Pune knowns as The Cosmos Co-operative Bank Ltd. had faced a cyber-attack in which a sum of Rs. 94 crore was drawn off the bank. The hackers stole the details of various account holders and drew money from the ATM machines. The crime was not limited to one country but around 28 countries from where the hacker group wiped off the money. Also, some amount of money was transferred through SWIFT in a bank account in Hong Kong.

3) Sony.sambandh.com Case[1]
In this case, a website known as sony.sambandh.com was used to commit fraud. This website was the platform through which the NRIs can purchase and deliver the products of Sony to their family & friends residing in India. The accused transacted through the credit card of an American citizen and made a delivery to himself. Later on the credit card company informed the Sony Co. about the denial of payment by the cardholder. A complaint was filed with the CBI against the accused named Arif Azim who was an employee in a call center. He acquired the details of the credit card through call and ordered the product. The court convicted him under Section 418, 419 & 420 of the IPC.

4) SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra[2]
This is one of the remarkable cases in which the Indian Court assumed jurisdiction in a matter regarding cyber defamation. The court in this case granted an injunction restraining the accused from defaming the aggrieved party through defamatory emails.

5) State of Tamil Nadu vs. Suhas Katti[3]
This case was related to posting of obscene and defamatory message about a divorced woman in a Yahoo message group. The accused also used a fake email account for the purpose of forwarding emails in the name of the victim which resulted in annoying phone calls to the victim in the belief that she was soliciting. The accused person was arrested by the police after making complaint in February, 2004 by the victim. This case is considered to be the first case of Tamil Nadu in which the offender was offender was convicted under Section 469 & 509 IPC and Section 67 of Information Technology Act, 2000. It is one of the landmark cases related to cyber-crime management in India.

6) bazee.com Case[4]
The CEO of the website 'bazee.com' was arrested in December, 2004 for selling Compact Disks (CDs) having offensive material on the website as well as in the markets of Delhi. The Mumbai Police and Delhi Police took action and arrested the accused but later on he was released on bail.

7) The Bank NSP Case
A management trained of a bank got engaged to a girl for marriage. The couple used to talk through email using the company's computer system. After some time, the marriage was broken and the girl created fake email IDs named "Indian Bar Association" and sent mails to the foreign clients of the boy. The Bank Company faced a huge loss and also the number of clients was compromised. The Bank was held liable for the emails sent using its computer system.

8) Andhra Pradesh Tax Case[5]
The Vigilance Department raided the house of a plastic firm owner in Andhra Pradesh and recovered a sum of Rs. 22 crore. They had given the owner an opportunity to explain the team regarding unaccounted money within 10 days.

The accused submitted 6000 vouchers to prove his innocence and the legality of trade. But after examining carefully, it was found that the vouchers were made after the raid. Further, it was revealed that the accused person was also running different businesses under the mask of one company & one business and for that purpose, he had made counterfeit vouchers to show sales record in order to escape tax liabilities.

Cyber Law in India

The Information Technology Act, 2000[6]
There are few noteworthy provisions in the Information Technology Act 2000 such as:

1) Section 65: Tampering with computer source documents[7]

[1] CBI Vs Arif Azim [(2008) 105 DRJ 721: (2008) 150 DLT 769]
[2] Suit No. 1279/2001, District Court of Delhi
[3] C No. 4680 of 2004
[4] Avnish Bajaj v. State (NCT) of Delhi (2008) 105 DRJ 721: (2008) 150 DLT 769
[5] https://www.indiancybersecurity.com/case_study_andhra_pradesh_tax_case.php
[6] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[7] Ibid Section 65

- Whoever knowingly or intentionally conceals, destroys or alters any computer source code used for a computer, computer programme, computer system or network.
- **Punishment**: A person charged under this provision shall be punished with imprisonment upto 3 years and fine upto 2 lakhs or both.

2) Section 66: Computer related offences[8]
- If any person, dishonestly or fraudulently, does any act referred in Section 43 of this Act
- **Section 43[9]**: Penalty and Compensation for damage to computer, computer system, etc.
- **Punishment**: A person charged under this provision shall be punished with imprisonment upto 3 years or fine upto 5 lakhs or both.

3) Section 66A: Punishment for sending offensive messages through communication service, etc.[10]

Any person who sends using a computer resource or a communication device:
- any information of offending or menacing character
- any information which is false and is sent for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will
- any electronic mail sent for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such mail.

Punishment: Any person convicted under this provision shall be imprisoned with a term upto 3 years and with fine.

4) Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device[11]
- Whoever dishonestly or receive any stolen computer resource or communication device knowing or having reason to believe the same.
- **Punishment**: Any person convicted shall be punished with imprisonment upto 3 years or with fine upto 1 lakhs or both.

5) Section 66C: Punishment for identity theft[12]
- Whoever, fraudulently or dishonestly uses the electronic signature, password or any other unique identification of a person
- **Punishment**: The person committing this crime shall be punished with imprisonment upto 3 years and also with fine upto 1 lakh rupees.

6) Section 66D: Punishment for cheating by personation by using computer resource[13]
- Whoever, by means of any communication device or computer resource cheats by personation.
- **Punishment**: Any person convicted under this section shall be punished with imprisonment upto 3 years and also with fine upto 1 lakh rupees.

7) Section 66E: Punishment for violation of privacy[14]
- Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person
- **Punishment**: A person held guilty in this section shall be punished with imprisonment upto 3 years or with fine not exceeding 2 lakhs or both.

8) Section 66F: Cyber Terrorism[15]

a) Whoever with an intent to threaten unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –
- denying or cause the denial of access to any person authorised to access computer resource; or
- attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
- introducing or causing to introduce any computer contaminant

Such act is likely to cause death or damage or harm to person or a property or affect the critical information infrastructure specified under Section 70 of this Act

b) Whoever intentionally or knowingly tries to gain access to unauthorized data which is limited or restricted for certain reason as it might cause injury to the interest on independence and integrity of India

Punishment: Any person who commits or conspires to commit cyber terrorism shall be punished with imprisonment for life.

9) Section 67: Punishment for publishing or transmitting obscene material in electronic form16
- Whoever transmits or publishes any obscene material which appears to be lascivious or likely to deprave or corrupt persons
- **Punishment**: Any person convicted for first time shall be imprisoned upto 3 years and with fine upto 5 lakhs and in case of second or subsequent conviction, he shall be imprisoned upto 5 years and with a fine upto 10 lakhs

10) Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form[17]
- Any person who publishes or transmits material containing sexually explicit content
- **Punishment**: Any person convicted for first time shall be imprisoned upto 5 years and with fine upto 10 lakhs and in case of second or subsequent conviction, he shall be imprisoned upto 7 years along with a fine upto 10 lakhs rupees.

[8] Ibid Section 66
[9] Ibid Section 43
[10] Ibid Section 66A
[11] Ibid Section 66B
[12] Ibid Section 66C
[13] Ibid Section 66D
[14] Ibid Section 66E
[15] Ibid Section 66F
[16] Ibid Section 67
[17] Ibid Section 67A

11) **Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form**[18]

- Any person who publishes or transmits material containing sexually explicit content depicting children
- **Punishment**: Any person convicted for first time shall be imprisoned upto 5 years and with fine upto 10 lakhs and in case of second or subsequent conviction, he shall be imprisoned upto 7 years along with a fine upto 10 lakhs rupees.

12) **Section 67C: Preservation and retention of information by intermediaries**[19]

- Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
- any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1)

Punishment: Any person who commits such offense shall be punished with imprisonment upto 3 years and also liable to fine

The Indian Penal Code, 1860[20]

The Indian Penal Code, 1860 and the Information Technology Act, 2000 are used in combination for the purpose of prosecuting the offender who commits identity theft and other related cybercrimes. Following are some provisions of IPC which deal with cybercrime:

1) Section 464: Making a false document[21]
2) Section 465: Punishment for forgery[22]
3) Section 468: Forgery for purpose of cheating[23]
4) Section 469: Forgery for purpose of harming reputation[24]
5) Section 470: Forged Document[25]
6) Section 471: Using as genuine a forged document or electronic records[26]

5. Conclusion

Cybercrimes are now becoming a popular crime which might have higher rate of destruction than Wars. Cyber warfare is the new generation of world War. The attention must be given to an individual who is more vulnerable to cyber threats and also for protecting his/her privacy in the cyberspace. Law must be enforced with deterrent punishment for criminals of such crime not only at national level but at international level too. Cybercrime in India is governed by the provisions of Information Technology Act of 2000. This law is proved to be very much effective against various types of Cybercrime committed within the nation as well as also has scope for the crime committed outside the nation. Awareness of Cybercrime and Cyber laws will be an effective step towards preventing this crime and the awareness must be done at grass-root level starting from the school.

[18] Ibid Section 67B
[19] Ibid Section 67C
[20] Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India)
[21] Ibid Section 464
[22] Ibid Section 465
[23] Ibid Section 468
[24] Ibid Section 469
[25] Ibid Section 470
[26] Ibid Section 471