Page 1288 - 1301 **DOI:** *https://doij.org/10.10000/IJLMH.114184*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 1

2023

Cyber Crime in India

DR. SURESH KUMAR[1] AND DR. KARAN SINGH GAUR[2]

ABSTRACT

Cybercrime refers to criminal activities that are carried out using the internet and other digital technologies. It is a rapidly growing concern worldwide and poses a significant threat to individuals, organizations, and governments. Cybercrime can take many forms, including hacking, identity theft, cyberstalking, online fraud, and cyberbullying, among others. In India, there have been increasing incidents of cybercrime, and it is becoming a major challenge for law enforcement agencies, the private sector, and the government. To address this issue, there is a need for a strong legal framework, enhanced technical capabilities, public-private partnerships, cyber security research, and the implementation of cyber security standards. Prevention and mitigation of cybercrime require a multi-stakeholder approach, where individuals, organizations, and the government work together to raise awareness, improve cyber security, and address the challenges associated with cybercrime. By being proactive and taking the necessary steps to protect themselves from cybercrime, individuals and organizations can help prevent and reduce the impact of this growing threat. This paper will be discussing the introduction, historical background of cybercrime, causes and challenges of cybercrime, types, laws, penalties, cases, and conclusion.

Keywords: *Cyber Crime, India.*

I. INTRODUCTION

Cybercrime refers to any illegal activity that is committed using the internet or other forms of digital communication technology. This includes a wide range of criminal activities such as hacking, phishing, cyber stalking, identity theft, cyber extortion, cyber bullying, and more. With the increasing use of technology and the internet, cyber-crime has become a global problem, affecting individuals, businesses, and governments alike. As technology continues to evolve, so do the methods used by cybercriminals, making it a constantly evolving and growing threat. To combat this growing problem, many countries have enacted laws and regulations to address cyber-crime and improve cyber security. However, the lack of technical expertise and public awareness still pose major challenges in effectively addressing and preventing cyber-crime. Cybercrime in India refers to illegal activities committed using the internet, computer systems,

[1] Author is an Assistant Professor at B.S. Anangpuria Institute of Law, Alampur, Faridabad, Haryana, India.
[2] Author is an Assistant Professor at B.S. Anangpuria Institute of Law, Alampur, Faridabad, Haryana, India.

 [ISSN 2581-5369]

or other digital devices. These crimes pose a significant threat to individuals, organizations, and the nation as a whole. Some of the common forms of cybercrime in India include:

Online Fraud: This includes scams such as phishing, where criminals impersonate a legitimate entity to steal personal and financial information.

Hacking: This involves unauthorized access to computer systems or networks to steal or manipulate data.

Cyber stalking: This refers to the use of digital devices to harass, intimidate, or threaten an individual.

Ransomware Attacks: This is a type of cyber-attack in which the attacker infects a computer system with malware and demands payment in exchange for access to the system.

The increasing use of technology in India has led to a rise in cybercrime cases, with individuals, small businesses, and large organizations alike falling victim. The government of India has taken steps to tackle cybercrime, including enacting stricter laws, setting up specialized police units, and promoting public awareness about safe internet usage practices. However, challenges still remain in investigating and prosecuting cybercrime cases, due to the technical nature of the crimes, limited technical capabilities of law enforcement agencies, and a shortage of cyber security experts.

II. HISTORICAL BACKGROUND CYBER CRIME

The history of cyber-crime can be traced back to the early days of the internet and computer networks.

- As soon as the internet became widely available in the 1980s and 1990s, it became a tool for criminals to commit various forms of illegal activities. One of the earliest recorded incidents of cyber-crime was the creation of a computer virus called "Brain" in 1986. Over the years, as technology has advanced and the internet has become more widespread, the types and frequency of cyber-crimes have evolved and increased.
- The 1990s saw the rise of hacking and phishing attacks, while the early 2000s saw an increase in identity theft and online fraud. The growth of social media and mobile technology in the late 2000s and early 2010s has led to the rise of cyber stalking, cyber bullying, and other forms of online harassment. With the increasing reliance on technology in everyday life, the threat of cyber-crime has only continued to grow, making it a major concern for individuals, businesses, and governments around the world.

 [ISSN 2581-5369]

III. CAUSES OF CYBER CRIME

There are several factors that contribute to the rise of cyber-crime:

Lack of Awareness: A lack of public awareness about cyber security and safe online practices can make individuals and organizations more vulnerable to cyber-attacks.

Technological Advancements: As technology continues to advance, cyber criminals are able to find new ways to carry out their illegal activities.

Weak Security Measures: Many organizations and individuals have weak security measures in place, making it easier for cyber criminals to gain access to sensitive information.

Profit Motive: Many cyber criminals are motivated by financial gain, and the anonymity of the internet provides them with a way to carry out their illegal activities without being detected.

Political or Ideological Motives: Some cyber criminals carry out attacks for political or ideological reasons, seeking to disrupt or damage a particular organization or government.

Insiders: In some cases, cybercrime is committed by employees or contractors who have access to sensitive information and use it for personal gain or to harm their organization.

Social Engineering: Cyber criminals use various tactics, such as phishing and social engineering, to trick individuals into revealing their personal information or installing malicious software.

IV. CHALLENGES OF CYBER CRIME

There are several challenges associated with addressing cybercrime in India, including:

Technical Challenges: The fast pace of technological development and the complexity of cybercrimes make it difficult for law enforcement agencies to keep up with the latest trends and techniques used by cybercriminals.

Lack of Skilled Personnel: There is a shortage of skilled personnel in India with expertise in cyber security, making it difficult for organizations to effectively protect themselves from cybercrime.

Cross-Border Nature of Cybercrime: The cross-border nature of cybercrime makes it difficult for law enforcement agencies to track and prosecute cybercriminals, as they can operate from different countries and jurisdictions.

Slow Legal Process: The legal process for dealing with cybercrime can be slow, with cases taking years to come to trial and resulting in few convictions.

 [ISSN 2581-5369]

To overcome these challenges, it is important for the Indian government and law enforcement agencies to work closely with the private sector and academic institutions to increase awareness, develop technical expertise, and improve the legal framework for dealing with cybercrime. It is also important for individuals and organizations to take a proactive approach to cyber security, by implementing measures to protect themselves from cybercrime and staying informed about the latest threats and trends.

V. KINDS OF CYBER-CRIME

There are several types of cybercrime, including:

Hacking: unauthorized access to or control over computer systems or networks.

Phishing: the use of fake emails or websites to trick individuals into revealing their personal information, such as passwords or credit card numbers.

Cyber stalking: using the internet or other digital communication technology to harass, intimidate, or threaten someone.

Identity Theft: stealing someone's personal information, such as their name, address, or Social Security number, to commit fraud or other crimes.

Cyber Extortion: threatening to release sensitive information or launch a cyber-attack unless a ransom is paid.

Cyber bullying: using the internet or other digital communication technology to harass, humiliate, or threaten someone, especially minors.

Online Fraud: using the internet to commit fraudulent schemes, such as selling fake products or using fake websites to steal credit card information.

Cyber Espionage: unauthorized access to sensitive or classified information by another nation or organization.

Crypto jacking: unauthorized use of someone's computer resources to mine crypto currency.

DoS Attacks: overwhelming a website or network with traffic to make it unavailable to users.

VI. CMPLAINT OF CYBERCRIME

In India, if you have been a victim of cybercrime, you can file a complaint with the following agencies:

Indian Computer Emergency Response Team (CERT-In): CERT-In is the national nodal agency responsible for responding to computer security incidents and providing technical

 [ISSN 2581-5369]

assistance to victims. You can report cybercrime incidents to them via their website or email (incident@cert-in.org.in).

The Cybercrime Reporting Portal: The government of India has set up an online portal for reporting cybercrimes. You can report the incident through this portal: https://cybercrime.gov.in/.

Local police: You can also file a complaint with your local police station. In case of a cybercrime emergency, you can also reach out to the National Critical Information Infrastructure Protection Centre.

VII. INVESTIGATION OF CYBER CRIME

The investigation of cybercrime in India is carried out by the law enforcement agencies, specifically the Cyber Crime Cells of various state police departments and the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI). These units are responsible for investigating cybercrime cases and working with other government agencies to prevent cybercrime and protect citizens. The Cyber Cell is a specialized unit within the law enforcement agencies of India that is responsible for investigating cybercrime cases. It works to prevent cybercrime, protect citizens from online threats, and bring cybercriminals to justice. The following are some of the key responsibilities of a Cyber Cell:

- **Receiving and investigating complaints:** The Cyber Cell receives complaints from individuals and organizations regarding cybercrime, and it investigates the cases to determine the extent of the crime and identify the perpetrators.
- **Gathering and analysing evidence:** The Cyber Cell gathers digital evidence from computers, mobile devices, and other digital devices and analyses the evidence to determine the methods used by the attacker.
- **Interrogation and arrest:** Based on the evidence, the Cyber Cell may question suspects and make arrests.
- **Prosecution:** The Cyber Cell works with the legal authorities to prosecute cybercriminals and bring them to justice.
- **Awareness and Prevention:** The Cyber Cell also works to raise public awareness about cybercrime and safe internet usage practices. It provides training and education to individuals and organizations to help them protect themselves from online threats. The Cyber Cell plays a crucial role in protecting citizens and organizations from cybercrime, and it works closely with other government agencies and international law enforcement

 [ISSN 2581-5369]

organizations to tackle these crimes.

- **Lodging a complaint**: The first step in investigating cybercrime is to file a complaint with the local police or a cybercrime reporting centre.
- **Technical Analysis:** Technical experts are often called upon to analyze the digital evidence and provide information on the methods used by the attacker.

It is important to note that the process of investigating cybercrime can be complex and time-consuming, and it is often challenging to track down and prosecute cybercriminals who operate from outside India. Despite the challenges, the Indian government is working to improve its capacity to investigate and prosecute cybercrime and to protect citizens from these crimes.

VIII. REMEDIES FOR VICTIMS OF CYBERCRIME

The remedies for victims of cybercrime vary depending on the nature and extent of the crime, but some common steps include:

Report the crime: Report the crime to law enforcement, the relevant websites or service providers, and any other relevant agencies.

Document evidence: Keep copies of any relevant emails, screenshots, or other evidence of the crime.

Change passwords: Change the passwords to any accounts that have been compromised.

Monitor accounts: Closely monitor your accounts and financial statements to detect any unauthorized activities.

Seek legal assistance: Consider seeking legal assistance to help you recover any losses and take action against the perpetrators.

Protect personal information: Take steps to protect your personal information and be cautious of unsolicited emails, calls, or messages.

Improve cyber security: Improve your cyber security by using strong passwords, enabling two-factor authentication, and regularly updating your security software.

Remember, it's important to act quickly and seek assistance from authorities to help minimize the impact of a cybercrime and prevent further harm.

IX. CYBER LAWS IN INDIA

The objectives of the cybercrime laws in India are to:

Protect citizens: To ensure that citizens have protection against online crimes, such as hacking,

identity theft, cyber stalking, and online fraud.

Regulate electronic commerce: To regulate electronic commerce and ensure the security and confidentiality of electronic transactions.

Preserve national security: To preserve national security and protect the country's critical information infrastructure from cyber-attacks.

Strengthen law enforcement: To provide law enforcement agencies with the tools and powers necessary to investigate and prosecute cybercriminals.

Foster a safe and secure online environment: To foster a safe and secure online environment for citizens and businesses, and promote the growth of the digital economy.

X. INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000, along with various rules and regulations, provides a comprehensive legal framework for addressing the issue of cybercrime in India and protecting the rights of individuals and organizations in the digital world. However, the effectiveness of the law depends on its implementation and enforcement, as well as the continued development of technology and the internet. The primary legislation governing cybercrime in India is the Information Technology Act, 2000, which has been amended several times to address emerging threats and challenges. The act provides a comprehensive legal framework for dealing with cybercrime, including provisions for punishment and compensation. Cyber law in India is governed by the Information Technology Act 2000, which was amended in 2008 to provide a comprehensive legal framework for electronic transactions and to address the issue of cybercrime in India. Some of the key provisions of the act include:

Legal Recognition of Electronic Documents: The act provides legal recognition to electronic records and digital signatures, making them equivalent to their paper-based counterparts.

Criminal Offenses: The act defines various cybercrimes, including hacking, identity theft, cyber stalking, and publishing obscene material, and provides for punishment for those who commit such crimes.

Data Protection: The act provides for the protection of sensitive personal data, such as financial information and health records, and imposes penalties on those who mishandle such data.

Intermediary Liability: The act provides guidelines for intermediaries, such as internet service providers, social media platforms, and websites, regarding their responsibility in the event of cybercrime committed through their networks.

 [ISSN 2581-5369]

Adjudication and Enforcement: The act provides for the establishment of special courts for the speedy trial of cybercrime cases, and for the appointment of cybercrime investigators to assist the police in such cases.

XI. PENALTIES CYBER CRIME IN INDIA

Under the Information Technology Act 2000 in India, the penalties for cybercrime can vary depending on the nature and severity of the crime. Some of the penalties for common cybercrimes in India include:

Hacking: Hacking is punishable with imprisonment for a "term that may extend up to 3 years, or a fine of up to two lakh rupees, or both."

Identity Theft: Identity theft is punishable with imprisonment for a "term that may extend up to 3 years, or a fine of up to two lakh rupees, or both."

Cyber stalking: Cyber stalking is punishable with imprisonment for a term that may extend up to 3 years, or a fine of up to two lakh rupees, or both.

Cyber Extortion: Cyber extortion is punishable with imprisonment for a term that may extend up to 3 years, or a fine of up to five lakh rupees, or both.

Cyber bullying: Cyber bullying is punishable with imprisonment for a term that may extend up to 3 years, or a fine of up to one lakh rupees, or both.

Online Fraud: Online fraud is punishable with imprisonment for a term that may extend up to 3 years, or a fine of up to five lakh rupees, or both.

Crypto jacking: Crypto jacking is punishable with imprisonment for a term that may extend up to 3 years, or a fine of up to five lakh rupees, or both.

The penalties for cybercrime in India can be severe, and it is important for individuals and organizations to take appropriate measures to protect themselves from such crimes. In addition to the legal penalties, the consequences of a cybercrime can include financial losses, reputational damage, and emotional trauma for the victims.

XII. CYBER CRIME PENALTIES UNDER INDIAN PENAL CODE, 1860

In addition to the penalties specified under the Information Technology Act 2000, several cybercrimes in India are also punishable under the Indian Penal Code (IPC). Some of the key provisions of the IPC relevant to cybercrime include:

Section 420: This section deals with cheating and dishonesty, and covers online fraud and other forms of cybercrime that involve deceit or false representation. Punishment for cheating under

 [ISSN 2581-5369]

the IPC is imprisonment for a term that may extend up to 7 years, or a fine, or both.

Section 468: This section deals with forgery, and covers crimes such as phishing, where criminals create fake websites or emails that look like legitimate ones, in order to steal sensitive information. Punishment for forgery under the IPC is imprisonment for a term that may extend up to 7 years, or a fine, or both.

Section 471: This section deals with using as genuine a forged document, and covers crimes such as using fake email addresses or identities to engage in illegal activities online. Punishment for using a forged document as genuine under the IPC is imprisonment for a term that may extend up to 7 years, or a fine, or both.

Section 499: This section deals with defamation, and covers crimes such as cyber stalking or cyber bullying, where criminals use the internet to harass or defame someone. Punishment for defamation under the IPC is imprisonment for a term that may extend up to 2 years, or a fine, or both.

XIII. CYBER CRIMES PENALTIES OTHER LAWS

In addition to the Indian Penal Code and the Information Technology Act, 2000, there are several other laws in India that provide penalties for cybercrimes. Some of the key laws include:

The Code of Criminal Procedure, 1973: This law provides for the procedure for investigating and prosecuting cybercrimes, and provides for the punishment of those who engage in such crimes.

The Electronic Transactions Act, 2000: This law provides for the legality of electronic transactions and the penalties for cybercrimes that involve unauthorized access or use of electronic records.

The Protection of Children from Sexual Offences (POCSO) Act, 2012: This law provides for the protection of children from sexual exploitation, including child pornography and child sexual abuse material.

The Unlawful Activities (Prevention) Act (UAPA), 1967: This law provides for the prevention of terrorism and other forms of organized crime, and covers cybercrimes that are committed in support of terrorist organizations or other criminal groups.

These laws, along with the Indian Penal Code and the Information Technology Act 2000, provide a comprehensive legal framework for addressing the issue of cybercrime in India, and imposing penalties on those who engage in such crimes. The penalties under these laws can be severe, and it is important for individuals and organizations to be aware of the risks and dangers

 [ISSN 2581-5369]

of the internet, and to take appropriate measures to protect themselves from cybercrime.

XIV. JUDICIAL CASES CYBER CRIME

There have been several high-profile cases of cybercrime in India that have been dealt with by the Indian courts. Some of the notable cases include:

Shreya Singhal v. Union of India: This case dealt with the constitutionality of Section 66A of the Information Technology Act, which imposed restrictions on free speech on the internet. The Supreme Court of India declared the section unconstitutional, stating that it violated the right to freedom of speech and expression guaranteed by the Indian Constitution.

Nasimuddin Siddiqui v. State of UP: This case dealt with the unauthorized access and misuse of personal data, and resulted in the conviction of the accused under the Information Technology Act.

Puneesh Kumar v. State of Haryana: This case dealt with the unauthorized interception of communication, and resulted in the conviction of the accused under the Indian Penal Code and the Information Technology Act.

Ravi Srinivasan v. Union of India: This case dealt with the defamatory tweets posted on Twitter, and resulted in the arrest and conviction of the accused under the Indian Penal Code.

XV. PREVENTION CYBER CRIME

Preventing cybercrime requires a combination of technical measures and user awareness. Here are some steps that individuals and organizations can take to prevent cybercrime:

Use strong passwords: Use a combination of letters, numbers, and symbols to create a password that is difficult to crack. Avoid using easily guessable information such as birthdays or family names.

Keep software up to date: Regularly update your operating system and other software to ensure that any vulnerability is patched.

Use antivirus software: Install and regularly update antivirus software to protect your computer from malware and other threats.

Be cautious with email attachments: Be wary of opening email attachments from unknown sources, as these may contain malware or other malicious content.

Use encryption: Use encryption to protect sensitive information, such as credit card numbers or confidential business information, when it is transmitted over the internet.

Enable two-factor authentication: Use two-factor authentication, where possible, to add an

 [ISSN 2581-5369]

extra layer of security to your accounts.

Educate employees: Train employees on the dangers of cybercrime, and the steps they can take to prevent it.

Develop a security policy: Develop a security policy that outlines the steps your organization will take to protect against cybercrime, and educate employees on how to implement it.

Awareness and Education: Raising public awareness about the risks associated with the internet and providing education and training on cyber security can help individuals and organizations protect themselves from cybercrime.

Strong Legal Framework: Implementing a strong legal framework, including clear laws and penalties for cybercrime can help deter potential cybercriminals and provide a basis for effective law enforcement.

Enhancing Technical Capabilities: Enhancing the technical capabilities of law enforcement agencies, including their ability to track and prosecute cybercriminals, can help them effectively deal with cybercrime.

Public-Private Partnership: Building strong partnerships between the government, private sector, and academic institutions can help share expertise, knowledge, and resources for addressing cybercrime.

Encouraging Cyber security Research: Encouraging research and development in the field of cyber security can help organizations and individuals stay ahead of the latest threats and trends.

Cyber security Standards: Implementing and enforcing cyber security standards for organizations and individuals can help ensure that systems and data are protected from cybercrime.

XVI. CONCLUSION

Cybercrime is a growing concern in India and poses a significant threat to individuals, organizations, and the economy. The rapid growth of technology and increased use of the internet have made it easier for cybercriminals to carry out their activities, and the cross-border nature of cybercrime makes it challenging for law enforcement agencies to track and prosecute them. However, there are several policies that can be implemented to address this issue, including raising awareness and education, strengthening the legal framework, enhancing technical capabilities, building public-private partnerships, encouraging cyber security research, and implementing cyber security standards.

 [ISSN 2581-5369]

It is important for individuals, organizations, and the government to take a proactive approach to cyber security and to work together to prevent and address cybercrime in India. By being aware of the risks associated with the internet and taking appropriate measures to protect themselves, individuals and organizations can help prevent and reduce the impact of cybercrime in India.

Cybercrime in India is on the rise and is becoming a major concern for individuals, organizations, and the government. The types of cybercrimes reported in India include online fraud, cyber stalking, hacking, identity theft, phishing scams, and ransom ware attacks. The increase in internet and smartphone usage has led to a surge in the number of cybercrime cases. The Indian government has taken several steps to tackle cybercrime, including enacting stricter laws, setting up specialized police units, and increasing public awareness about safe internet usage practices. However, the challenges faced in investigating and prosecuting cybercrime cases remain significant due to the technical nature of the crimes, limited technical capabilities of law enforcement agencies, and a shortage of cyber security experts.

*****

 [ISSN 2581-5369]

XVII. REFERENCES

- Mark Stanislav and Caleb Sima, Cybercrime and Digital Forensics: An Introduction (Jones & Bartlett Learning, 2015).
- Mark D. Rasch, Cybercrime: The Investigation, Prosecution and Defence of a Computer-Related Crime (Jones & Bartlett Publishers, 2008).
- Orin S. Kerr, Computer Crime Law (Aspen Publishers, 2010).
- Eoghan Casey, Digital Evidence and Computer Crime (Elsevier, 2011).
- Steven Wilson, Cybercrime: Criminal Threats from Cyberspace (Praeger, 2009)
- Mark J. Lanterman, The Law of Cybercrimes and Their Investigations (Jones & Bartlett Publishers, 2012)
- Dawn C. Nunziato, Cybercrime: A Reference Handbook (ABC-CLIO, 2009)
- Peter Grabosky, Computer and Internet Crime (Cambridge University Press, 2006)
- V.S. Malimath and H.K. Sardana, Cybercrime Law in India: Issues and Challenges (LexisNexis, 2015)
- Sujatha Mukherjee and Shweta Bhatt (eds.), Cybercrime in India: Issues and Challenges (Deep & Deep Publications, 2012)
- B.S. Sial, Cybercrime and Cyber security in India (Sage Publications, 2017)
- Bhaskar Mukhopadhyay, Cybercrime, Cyber law and Cyber security in India (Deep & Deep Publications, 2017)
- Usha R. Medury and Priyadarshini Nag, Cybercrime: An Overview of its Impact in India (Atlantic Publishers & Dist, 2018)
- S.K. Karn, Cyber Laws in India: A Practical Guide (LexisNexis, 2017)
- J.K. Dass and P.K. Tiwari, "Cybercrime in India: A Review" International Journal of Engineering and Technology (2015)
- S.K. Kar, "Cybercrime and its Implications in India" (Journal of International Criminal Justice (2013)
- B.S. Sial, "Cybercrime and Cyber security in India: An Overview" (Indian Journal of Criminology and Criminalistics, 2017)

 [ISSN 2581-5369]

- A.S. Narayanan and S.K. Saini, "Challenges in Combating Cybercrime in India" Journal of Cyber security (2015)
- Usha R. Medury and Priyadarshini Nag, "Investigating Cybercrime in India: An Analysis of Key Challenges" Journal of Cybercrime and Digital Evidence (2018)

*****

 [ISSN 2581-5369]