International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 566-571 www.ijaem.net ISSN: 2395-5252

# An examination of the concept of cybercrimes under Indian criminal law with particular reference to the Information Technology Act of 2000

Md Jiyauddin[1], Sunita Banerjee[2]
[1,2]*Assistant Professor, School of Law, Vel Tech Rangarajan DrSagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India.*

Date of Submission: 07-04-2024 Date of Acceptance: 17-04-2024

**ABSTRACT**
The concept of crime is fundamentally concerned with social order. It is commonly understood that man's interests are best served as a member of the community. Everyone owes some obligations to his fellow men while also having certain rights and privileges that he expects others to protect. This attitude of mutual respect and confidence in others' rights governs the behaviour of society members as a whole. Although most individuals believe in the 'live and let live' philosophy, there are a minority who, for whatever reason, stray from this usual behavioural pattern and engage in anti-social activities. This clearly lays a duty on the state to maintain social order. Crime appears to have evolved in tandem with the changes in social circumstances that occurred throughout human society's developmental phases. As a result, it is clear that the idea of crime is inextricably linked to current social policies. The definition of crime evolves alongside ideological shifts. That is, certain new crimes emerge while certain previous crimes become outdated, and they are dealt with completely by making appropriate adjustments to the criminal legislation. As a result, criminal law is frequently used as a barometer to assess the moral turpitude of society. In light of various laws under the Information Technology Act 2000, Indian Penal Code 1860, Code of Criminal Procedure 1973, Indian Evidence Act 1872, and by analysing judicial patterns, the researcher attempts to identify the facts and concerns, and makes some recommendations to address the difficulties of cybercrime.

**KEYWORDS:** Crime, Anti-Social Activities, Criminal legislation, Information Technology, Indian Penal Code, Code of Criminal Procedure.

## I. INTRODUCTION

The rapid development of information technology, particularly the Internet and electronic media, since the 1980s has resulted in a new breed of computer-related crimes known as 'cyber-crimes'. The vast proliferation of these crimes has become a source of worldwide worry and a problem for law enforcement organisations in the new millennium. Because of the unique nature of these crimes, they may be done anonymously and from a distance without physically being there. Furthermore, hackers have a significant advantage: they may utilise computer technology to cause damage without fear of being detected. These crimes encompass a wide range of illicit computer-related acts, including theft of communication services, industrial espionage, electronic money laundering and tax evasion, electronic vandalism, cyber terrorism, and the transmission of pornographic and objectionable information in cyberspace. Cybercrime is a crime that involves the use of the Internet. The Internet is not a physical or actual object, but rather a vast network that links countless tiny groupings of linked computer networks. It is therefore a network of computer networks designed to exchange data and communications. The Internet refers to the worldwide web of linked networks and computers. Billions upon billions of people throughout the world today use the Internet for a variety of reasons, including education, entertainment, e-shopping, and e-governance.

The computer and network of Information Technology (IT) have become an essential element of everyday life. It is both a blessing and a curse. The overuse of information technology has a bad aspect as well. It has created new chances for crooks and antisocial elements. They are more

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 566-571 www.ijaem.net ISSN: 2395-5252

capable of expanding their illegal operations in the cyber world. They are new and use very sophisticated methods of breaching the law. They may now use the Internet to commit classic crimes such as slander and pornography. Regulation and control of cyberspace have become critical since a big number of terrorist organisations throughout the world are now utilising the Internet to carry out terrorist actions, endangering the peace and tranquilly of society and diverse nations.

## II.SIGNIFICANCE

Nowadays, computers and the Internet touch and affect nearly every area of our life. We live in the information era, and computers are the driving force behind our existence. We rarely engage in any activity that is not in some way dependent on computers. From the minute we wake up until we fall asleep, we interact with computers. The place we live in, the power we consume, the transportation we use, the water we drink, our healthcare records, our government, our banking, and our entertainment are all dependent on and, in some cases, influenced by computers. As a result, we must not only be computer literate, but also comprehend the myriad challenges surrounding our widespread and necessary reliance on computers.

The Internet offers intellectual property owners an apparently limitless market for their creations. At the same time, the Internet expands chances for individuals wishing to infringe on the rights of others, making discovery and eradication increasingly difficult. The difficulty that the law has faced in recent years has been how to encourage the growth of intellectual property on the Internet while limiting its unauthorised use. The research focuses on numerous facets of cyberspace, including the criminal activities that influence people's daily lives and the efforts that may be taken to avoid cybercrimes.

## III. OBJECTIVES

- To examine the idea, nature, and extent of cybercrime.
- To analyse various actions of cybercrime.
- To present some tips for preventing cybercrime in India.

## IV. CYBERCRIME AND COMPUTER CRIME

1. **Computer crimes**: The term 'computer crimes' refers to the abuse of computers and their networks. It's one of the oldest and most widely used terms. There are numerous behaviours that are not illegal under existing laws and should be included in the definition of 'computer crime'. It is not necessary to have extensive computer skills in order to commit a computer crime. Because of the fast advancement of information technology, even non-technical people can conduct cybercrimes.

2. **Information Technology Crimes**: Some authors use the phrase "Information Technology Crimes" to denote the role of technology in criminal conduct. Others use the phrase 'high-tech crimes' to describe illegal behaviour involving computers and satellite communication systems. The word "information technology" refers to a wide range of services, including computers, Internet services, satellite usage, e-mail services, and other ways involving the use of any communication device, such as a mobile phone.

3. **Computer-related crimes**: The term 'computer-related crimes' was discovered to be in widespread use during the early days of computers. The word refers to computer-related crimes such as software piracy or hacking.

4. **Tele communication crimes**: Since the introduction of mobile phones, the Internet, and the World Wide Web, the distinction between computer technology and telecommunications technology has been blurred. The telecom system communicates with the computer and vice versa. The term 'telecom crimes' has so lost its meaning in the current context. It is confined to small offences such as the theft of cables, poles, and telecom equipment, as well as the intentional damage to equipment.

5. **Cybercrimes**: The widespread use of the Internet and computer networks in everyday life has made computer-related crimes a topic of fascination among the general public and the media, and the simple phrase 'cybercrime' has captured people's imaginations. Anything connected to the Internet and computer networks was given the prefix 'cyber', and a slew of new terms emerged, including cyber laws, cyber cafes, cyber police, cyberspace, cyber stalking, and cyber technology. The information in cyberspace simply refers to activity in the virtual world.

6. **Computer crimes get a new name: cybercrimes**: A cybercrime may be described

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 566-571 www.ijaem.net ISSN: 2395-5252

as "the act of creating, distributing, altering, stealing, misusing, and destroying information through computer manipulation of cyberspace without the use of physical force and against the victim's will or interest."66 The term 'cybercrime' refers to any types of disagreeable or criminal behaviours, misuse, or abuse that occur in the cyber world or through or against computer networks or telecom networks that run on a computer system. The definition of the word may change depending on the facts and circumstances of a particular situation. The scope of cybercrime is only going to expand as technology develops.

## V. SIGNIFICANT SECTIONS OF THE ACT

The IT Act is an important part of the Indian legal structure since it governs the whole investigation process for cybercrime. The applicable parts are listed below.

• Section 43 of the IT Act applies to those who commit cybercrime, such as harming a victim's computer without their consent. If a computer is broken without the owner's consent, the owner is entitled to a full reimbursement.

In Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others (2018), Rajesh Aggarwal of Maharashtra's IT department (representative in the current case) directed Punjab National Bank to pay Rs 45 lakh to Manmohan Singh Matharu, MD of Pune-based business Poona Auto Ancillaries. In this case, a fraudster deposited Rs 80.10 lakh from Matharu's PNB account in Pune after the latter responded to a phishing email. Because the complaint reacted to the phishing email, they were requested to share the blame. However, the bank was ruled responsible since no security checks were performed on bogus accounts created to deceive the Complainant.

• Section 66 applies to dishonest or fraudulent behaviour as specified in Section 43. In such cases, the penalty may be up to three years in jail or a Rs. 5lakh fine.

In Kumar v. Whiteley (1991), throughout the inquiry, the accused acquired unauthorised access to the Joint Academic Network (JANET) and removed, added, and modified files. According to investigations, Kumar was signing on to a BSNL broadband Internet connection as if he were an authorised legal user and changing computer databases including broadband Internet user accounts of customers. After discovering unauthorised usage of broadband Internet on Kumar's PC, the CBI filed a cybercrime case against him and conducted investigations based on an anonymous allegation. Kumar's unlawful behaviour also cost the subscribers Rs 38,248. N G Arun Kumar was punished by the Additional Chief Metropolitan Magistrate. The magistrate sentenced him to one year in jail and a Rs 5,000 fine under Sections 420 of the IPC and 66 of the IT Act.

• Section 66B outlines penalties for fraudulently receiving stolen communication devices or computers, including a potential three-year jail sentence. Depending on the severity, a fine of up to Rs. 1 lakh may be levied.

• Section 66C addresses digital signatures, password hacking, and other kinds of identity theft. This clause sanctions imprisonment for up to three years and a fine of one lakh rupees.

• Section 66D addresses cheating through computer resources. If found guilty, the punishment can range from three years in prison to a fine of up to Rs 1 lakh.

• Section 66E penalises taking and publishing images of private parts without authorization. If found guilty, the penalties can range from three years in prison to a fine of up to Rs 2 lakh.

• Section 66F addresses cyber terrorism. A person convicted of a crime faces up to life in jail. For example, a threat email was sent to the Bombay Stock Exchange and the National Stock Exchange, challenging the security personnel to avert a terror assault on these institutions. The offender was captured and charged under Section 66F of the Information Technology Act.

• Section 67: This entails electronically publishing obscenities. If convicted, the prison term is up to five years and the fine is up to Rs 10 lakh.

## VI. PREVENTION OF CYBERCRIMES

Prevention of crime is more important than its detection, after it has occurred. In physical world, the police prevent crime through various steps like patrolling, rushing on emergency calls, guarding of vital installations and by providing security cover etc. But these strategies are neither practicable or desirable in the online. Another problem is that, many of the social norms and ethics which function as a deterrent to the commission of crime in physical world are either non -existent or inadequately developed for behaviour over the net.If the Internet is acknowledged as a worldwide means of communication and a free exchange of ideas, any preventative measures must be minimum, least obstructive, and acceptable in a democratic society.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 566-571 www.ijaem.net ISSN: 2395-5252

A)**Creating societal awareness**

Almost everyone, from all walks of life, uses computers or the Internet in some way. As a result, raising public knowledge about cybercrime is a vital step towards prevention. Teenagers' understanding of the negative repercussions of cybercrime, particularly pornography on the Internet, mobile phones, and other devices, is extremely beneficial in schools, universities, and cyber cafes. Active support from parents, teachers, and social workers is also beneficial in this area.

B) **Technology for preventing cybercrimes**

Cybercrimes are technology-based, they may be avoided by adopting electronic technology. Internet browsers can be set to prohibit users from entering the same password several times. Programming code can prohibit access to specific websites. Encryption is another one method for preventing cybercrimes.

C) **Deterrence as a preventative strategy**

Cybercrimes are regularly perpetrated by criminals because they are simple to commit, the offender's identity is preserved, and the crime takes place at a remote location around the world. Deterring tactics can also help prevent cybercrime. The IT Act 2000 and other criminal laws, such as the IPC 1860, offer suitable consequences for these offences. Investigation of cybercrimes was a significant difficulty a few years ago, but with the improvement in the training of cyber police, effective and correct investigation tactics are utilised by the investigation agencies, and therefore cybercrimes may be properly investigated presently.

## VII. CHALLENGES CAUSED BY CYBERCRIMES

Most nations have laws in place to pursue cybercrime. The criminal law would be unaffected in the absence of an extradition convention between the countries. Not only that, but to carry out an extradition treaty for the surrender of criminals, the relevant act of cybercrime must generate criminal culpability in the nation engaged in the treaty.

**Technical challenges**

When a cybercrime is committed on the Internet, the investigating agencies must identify the perpetrator, which requires the police to trace the crime from victim to offender. However, tracing an offender in cyberspace is difficult if the offender attempts to conceal his identity, if there are technical difficulties that impede the investigation, or if international cooperation is required. We all know that cybercrimes are borderless, sophisticated crimes that are easy to commit. The Internet's inherent transnational nature protects against police and allows criminals to commit cybercrimes safely. Cybercriminals might use techniques while communicating through Internet service providers, resulting in a challenging situation for investigative authorities. Bilateral legal aid between governments entails the sharing of evidence between the victim's and criminal's countries. If this procedure results in a time delay, the concrete electronic evidence may be destroyed or unavailable to investigative agencies. As a result, tracking the transmission of an alleged offence must be done in real time, during the commission itself. However, this is problematic owing to a lack of technology. While some fraudsters may leave electronic traces, others do not. Tracing cybercriminals is becoming increasingly difficult as offenders use anonymous software. Cybercriminals may conceal their illegal activity owing to the anonymous nature of cybercrime. This entails the use of omnipresent internet cafés, pre-paid cards that allow for anonymous communication, and so on. As a result of technical improvements in the electronic field, cybercrime has increased at a rapid pace.

**Legal difficulties**

The intrinsic international network of cybercrimes has rendered the old idea of distance irrelevant, allowing criminals to perpetrate them more readily. As a result, cybercriminals are committing crimes all over the world, causing unfair losses to individuals and profiting illegally for themselves. They also pose a threat to national security through actions such as hacking into vital defence institution websites and banks. Cybercriminals must be investigated and prosecuted using a capable legal system and a deterrent strategy. Cybercrime laws are equally vital for gathering evidence that may be used in court.

**Operational changes**

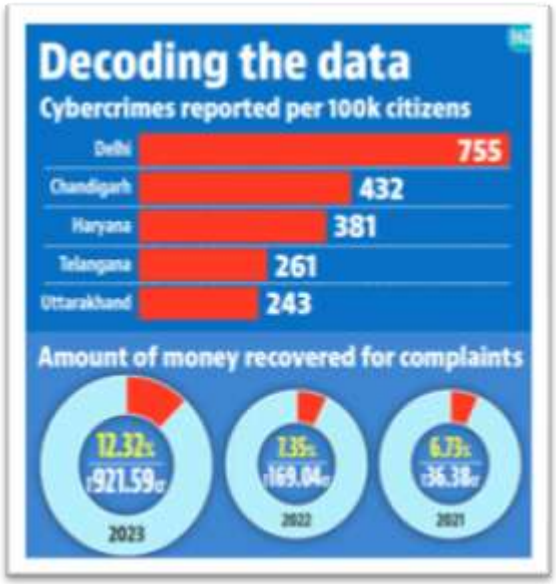
Personnel involved in the investigation and prevention of cybercrime must have a thorough understanding of electronics and communication technology. The government solicitors must review case legislation. Proceedings involving cybercrime will be brought before the Court of Law. Cyber forensic capabilities, which are critical in computer crime investigations, must be enhanced. Police personnel, attorneys, and judges must be adequately trained in the effective prosecution of

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 566-571 www.ijaem.net ISSN: 2395-5252

cybercrimes. Cybercrime poses significant challenges to law enforcement, which can be addressed by acquiring full technical knowledge of information technology and the law. The legal challenge can be removed by redefining existing criminal laws, and the operational challenge can be met by establishing a strong network of capable individuals in the fields of electronic technology and cyber forensics.

**In 2023, Delhi has the greatest number of per capita cybercrime complaints**

According to data given by CEO Rajesh Kumar on Wednesday, Delhi had the greatest amount of cybercrime complaints in the country, with 755 incidents filed per 100,000 inhabitants in 2023. Chandigarh has the second-highest rate (432), followed by Haryana (381) and Telangana (261). The hotline number 1930 has been linked with over 263 banks, e-commerce businesses, and other entities. Between 2021 and 2023, □ 1,127 crore was recovered for 430,000 victims. "This system was able to block this money within the financial channels so that increased the chances of recovery," Kumar went on to explain. Both the percentage and the total amount of money recovered have continuously climbed.




## VIII. CASE LAWS

Union of India (UOI) vs. G.S. Chatha Rice Mills and Others (MANU/SC/0714/2020) The provisions in the Customs Act governing the electronic presentation of the bill of entry for home consumption and self-assessment must be read in light of Section 13 of the Information Technology Act, which recognises "the dispatch of an electronic record" and "the time of receipt of an electronic record." The legal regime governing the electronic presentation of documents, such as the presentation of a bill of entry, has gained clarity as a result of the Information Technology Act's enabling framework, under which these data are preserved. Presentation of the Bill of Entry Section 46 is produced electronically and timestamped in accordance with the provisions of the Information Technology Act and Rule 5(1) of the Information Technology (Electronic Service Delivery) Rules 2011.

The State of Uttar Pradesh vs. Aman Mittal and Others. 2019(19) SCC740 The question was whether an obscene action arising from an electronic form would be criminal under Section 292 of the Indian Penal Code, Section 67 of the IT Act, or both, or under any other IT Act provision. This Court ruled that while Section 292 of the Indian Penal Code makes it a crime to sell obscene literature, etc., if the offence has a nexus or connection with an electronic record, the protection and impact of Section 79 cannot be ignored or negated in light of a unique provision for a specific purpose. The IT Act must be implemented to ensure that the protection is effective and faithful to the legislative meaning.

Christian Louboutin SAS v. Nakul Bajaj & Ors. (2018), 253 DLT 728

Facts: The Complainant, a luxury shoe maker, filed a lawsuit seeking an injunction against an e-commerce site, www.darveys.com, for engaging in trademark infringement with a seller of counterfeit goods.The Court's inquiry was whether the defendant's use of the plaintiff's mark, logos, and picture was protected under Section 79 of the IT Act.

Decision: The Court found that the defendant is more than an intermediary since the website has complete control over the items supplied through its platform. It first identifies and then encourages third parties to market their items. The Court further stated that active involvement by an e-commerce platform would exclude it from the rights granted to intermediaries under Section 79 of the IT Act.

## IX. CONCLUSION

In conclusion, recent advancements in computer networking and technology have led to an increase in cybercrimes. This poses a significant threat to humanity since attackers can target known victims with evil motives. Committing computer crimes includes inflicting harm, stealing or wiping data, altering passwords, and hacking credit card and bank account information. Cybercrimes such as

stalking, terrorism, pornography, morphing, forgery, email spoofing, and identity theft have significant societal repercussions. A cybercriminal can get unauthorised access to a victim's computer or personal information by hacking their account. Individuals must be aware of these crimes and keep attentive to prevent personal or professional losses.With humans' increasing reliance on technology, cyber laws in India and throughout the world must be constantly updated and refined to stay current. As a result of the epidemic, the number of remote workers has expanded significantly, emphasising the importance of application security. Legislators must take extra steps to stay ahead of imposters and take action against them as soon as they appear. It may be avoided if politicians, internet service providers, banks, shopping websites, and other intermediaries collaborate. However, in the end, it is up to users to help combat cybercrime. The only approach to increase online safety and resilience is to evaluate these stakeholders' behaviour and ensure they follow cyberspace law.

The legislative reaction to these concerns has been the development of extensive cyber legislation, principally embodied in the Information Technology Act of 2009. The Act establishes a legislative foundation for combating cybercrime and creating a safe digital environment. It includes rules for defining offences, conducting investigations, and imposing punishments on offenders. There are still hurdles to successful implementation and enforcement. Issues such as the dynamic nature of cyber threats, jurisdictional complications, and the need for regular revisions to keep up with technology improvements provide ongoing difficulties to the legal system. The report emphasises the necessity of international coordination in combating cybercrimes, which frequently cross-national borders. Building connections with other countries and international organisations is critical for a better coordinated and effective response to cyber threats. While India has made tremendous progress in building a legislative framework to tackle cybercrime, there is still a need for flexibility and adaptation. Regular legislative updates, greater law enforcement capabilities, and more public knowledge are all critical components of a holistic plan for mitigating cyberspace dangers.

## REFERENCES

[1]. S. Thangamayan and Murugan Ramu, “Cyber Crime and Cyber Law’s In India: A Comprehensive Study with Special Reference to Information Technology,”International Journal on Recent and Innovation Trends in Computing and Communication, x(y).

[2]. Bajpai, A., and Singh, P. (2020), "An Analytical Study of Cyber Laws in India." Journal of Cybersecurity and Information Management, 1(1), 35-50.

[3]. Kannabiran, G. (2019). "Cybercrime in India: Legal Challenges and Solutions." Journal of Cybersecurity and Privacy, 2(1), 45-62.

[4]. Niha Khan and Vaibhav Raj Singh, (2023), “AN ANALYTICAL STUDY OF SOCIAL MEDIA AND INDIAN CYBER LAW WITH IT’S PROBLEMS AND SOLUTIONS,” GRADIVA REVIEW JOURNAL, 9(6), 694-702.

[5]. Pallavi Kapila, (2020), “Contemporary Issues and Challenges in the Society,” New Era International Imprint, Edition: 2020,36-48.

[6]. Sakshi and Archana Vashishth, (2022), “An Analysis of Cyber Crime with Special Reference to Cyber Stalking,” Journal of Positive School Psychology, 6(4),1279-1287.

[7]. Jatin Patil, 2022, “CYBER LAWS IN INDIA: AN OVERVIEW,” Indian Journal of Law and Legal Research, 4(1), 1391-1411. https://doi-ds.org/doilink/02.2022-31571548/IJLLR/V4/I1/A132.