



## Research Article

# The Rising Threat of Cyber Crimes in India: Challenges, Legal Provisions, and Solutions

**Divyani Varma<sup>1\*</sup>, Dr. Richa Shrivastava<sup>2</sup>, Dr. Niti Nipuna<sup>3</sup>, Dr. Vishal Sharma<sup>4</sup>**

<sup>1</sup>Student, Institute of Law and Legal Studies, Sage University, Indore, Madhya Pradesh, India


<sup>2</sup>Associate Professor, Institute of Law and Legal Studies, Sage University, Indore, Madhya Pradesh, India

<sup>3</sup>HOD (Law), Institute of Law and Legal Studies, Sage University, Indore, Madhya Pradesh, India

<sup>4</sup>HOI (Law), Institute of Law and Legal Studies, Sage University, Indore, Madhya Pradesh, India

**Corresponding Author:** \*Divyani Varma

**DOI:** <https://doi.org/10.5281/zenodo.14946611>

Abstract	Manuscript Information
<p>This Research Paper will discuss the growth, nature, causes, and legal framework of cybercrime in India. It identifies the contribution of technology, business practices, and governance in preventing these crimes and suggests strategies to reduce their harm. While this study cannot provide evidence or definitive answers to the above questions, it hopes to shed light on the concerns that cybercrime affects everyone, whether it is their own business, company, or country. Cybercrime in India is on the rise due to rapid digitalization and widespread internet usage. This paper provides an in-depth look at the various types, causes, effects and legal frameworks of cybercrime in India. It highlights the challenges faced by law enforcement agencies and suggests effective ways to respond to cyber threats while preserving privacy and security.</p>	<ul style="list-style-type: none"> <li>▪ <b>ISSN No:</b> 2583-7397</li> <li>▪ <b>Received:</b> 19-01-2025</li> <li>▪ <b>Accepted:</b> 09-02-2025</li> <li>▪ <b>Published:</b> 27-02-2025</li> <li>▪ <b>IJCRM:</b>4(1); 2025: 176-181</li> <li>▪ <b>©2025, All Rights Reserved</b></li> <li>▪ <b>Plagiarism Checked:</b> Yes</li> <li>▪ <b>Peer Review Process:</b> Yes</li> </ul>
	<p><b>How to Cite this Article</b></p> <p>Varma D, Shrivastava R, Nipuna N, Sharma V. The rising threat of cyber crimes in India: challenges, legal provisions, and solutions. Int J Contemp Res Multidiscip. 2025;4(1):176-181.</p>
	<p><b>Access this Article Online</b></p>  <p><a href="http://www.multiarticlesjournal.com">www.multiarticlesjournal.com</a></p>

**KEYWORDS:** Cybersecurity in India, Information Technology Act, 2000, Indian Penal Code and Cyber Crimes, Data Protection Bill India, Digital Evidence and Cyber Law

## 1. INTRODUCTION

### Definition of Cybercrimes

Cybercrime encompasses any crime committed on the internet or other digital platforms. These cybercrimes include hacking, identity theft, cyber fraud, cyber stalking, and cyber terrorism.

Cybercrime refers to crimes committed using computers and the internet. As India's digital economy has grown over the past few years, cybercrime has also become a major concern. Financial fraud, identity theft, and cyber stalking are concerns in India. The purpose of this review is to identify trends, challenges and

responses to cybercrime in India. Cybercrime encompasses any crime involving computers or the internet. Examples include theft, identity theft, online bullying, online fraud and more serious crimes such as data breaches, cyber terrorism and property theft. The increasing reliance on technology has led to an increase in cybercrime in India.

### Background

As India becomes a global hub for IT services and digital innovation, cyber threats to the country are also increasing. Cybercrimes include financial fraud, identity theft, ransomware, online searches, and data breaches. India's rapid digitization has made it increasingly dependent on technology for communication, business, and governance. These developments also make it vulnerable to identity theft, phishing attacks, and even cybercrime.

### Problem Statement

The increasing dependency on digital platforms has also increased the vulnerability of individuals, businesses and governments to cyberattacks. There are many threats in the cyber world and although technology continues to advance, regulatory and administrative processes lag behind and these threats continue to increase. India is one of the largest digital economies and therefore faces unique challenges in this regard. While digital transformation has brought about advancements in almost every sector, it has also created vulnerabilities in cybersecurity. India is experiencing financial fraud, identity theft, phishing attacks and even ransomware, cybercrime and data breaches big. What is missing in this context is an understanding of the dynamics of cybercrime in India's economic and technological sectors, and therefore requires serious research and recommendations on how to effectively combat cybercrime.

## 2. OBJECTIVE OF THE RESEARCH

This study will lead to a better understanding of the legal framework for cybercrime in India. Some legal, regulatory and procedural issues in prosecuting or defending against criminal acts will be examined.

- Assess the adequacy of existing cybersecurity architecture and policies.
- Critically analyze the trends and patterns of cybercrime in India.
- Assess the legal framework against cybercrime in India. explain.
- Provide recommendations to reduce cybercrime.

## 3. LITERATURE REVIEW

Numerous scholars and researchers have studied the increasing cyber threats in India and the countermeasures required to tackle them. Kshetri (2019) analyzed India's rapid adoption of digital payment systems and found that while digital transactions enhance financial inclusion, they also create vulnerabilities in cyber security. The study highlighted how cybercriminals exploit weak authentication mechanisms and loopholes in digital infrastructure to commit financial fraud.

Bansal & Arora (2021) discussed the role of artificial intelligence (AI) in cybercrime prevention. Their research explored how AI-powered security systems can detect unusual network behavior, predict cyber-attacks, and automate threat responses. They concluded that AI-driven cybersecurity measures significantly improve threat detection capabilities but require continuous advancements to counter evolving cyber threats. Sharma *et al.* (2022) conducted a comprehensive study on India's cyber laws and their effectiveness in addressing cyber crimes. Their findings indicated that while the Information Technology Act, 2000, provides a legal framework, the enforcement of cyber laws remains weak due to inadequate resources and lack of awareness among law enforcement agencies. The study recommended stronger regulatory mechanisms and the implementation of more stringent penalties to deter cyber criminals. Gupta & Malhotra (2023) focused on the psychological impact of cybercrimes on victims. Their study revealed that cybercrimes such as identity theft, online harassment, and financial fraud lead to significant emotional distress and loss of trust in digital platforms. They suggested the need for psychological counseling services and awareness campaigns to help victims cope with the consequences of cybercrimes. Verma (2023) examined global best practices in cyber security and their applicability in India. His research suggested that India should adopt a multi-layered cybersecurity approach, similar to leading cyber-secure nations such as the United States and Estonia. He emphasized the importance of public-private partnerships, cyber education programs, and strict data protection laws to build a resilient cyber ecosystem. These studies collectively indicate that cyber threats in India are multifaceted and require a combination of legal, technological, and awareness-driven strategies to mitigate their impact. While India has taken significant steps to strengthen its cyber security framework, continuous efforts are needed to stay ahead of emerging cyber threats.

### Hypothesis

Cybercrime in India has become widespread due to the rapid advancement of technology, lack of cybersecurity training, and gaps in the legal system and governance that make it difficult for law enforcement agencies to combat these crimes.

The idea is that as more Indians and businesses engage with digital platforms, cybercriminals will start taking advantage of the lack of cybersecurity knowledge, inadequate legislation, and regulatory issues. Hopefully, these challenges will diminish over time as they are addressed through better training, stricter regulations, and improved governance and processes.

## 4. RESEARCH METHODOLOGY

**Research Design:** This study employs a mixed-methods approach, combining quantitative and qualitative data to achieve a holistic understanding of cybercrimes in India.

### Data Collection Methods

#### 1. Primary Data

**Surveys and Questionnaires:** An online survey was conducted for individuals, businesses, and IT professionals to understand

their experiences and knowledge of cybercrime. The survey will be organized and made available to IT professionals, law enforcement and the public. These services will collect information, experience and understanding of cybercrime.

**Interviews:** Semi-structured interviews were conducted with cybersecurity experts, law enforcement officials, and policy makers. In-depth interviews will be conducted with cybersecurity experts, legal experts, and cybercrime victims to understand the challenges and gaps in the current system.

## 2. Secondary Data

**Reports and Databases:** Review cyber security reports from organizations such as CERT-In, NASSCOM and international organizations.

**Legal Case Studies:** To examine the outcomes of major cybercrime cases and prosecutions in India. To identify vulnerabilities and response mechanisms by analyzing major cybercrime incidents in India.

**Policy Documents:** India's cyber security policy and examination of international benchmarks.

**Literature Review:** Review of academic literature, government publications and policy documents on cybersecurity and cybercrime in India.

**Statistical Data:** Use of data from organizations such as the National Crime Records Bureau (NCRB), CERT-In (Indian Computer Emergency Response Team), and international cybersecurity firms to track trends and patterns.

## Sampling

The study employs stratified random sampling to ensure diverse representation from urban, semi-urban, and rural populations, alongside different economic and professional backgrounds.

## Data Analysis

Quantitative data will be analyzed using statistical tools to identify trends, patterns, and correlations, while qualitative data will undergo thematic analysis to extract insights and narratives.

## Significance of the Study

Apart from the government, this research is equally pertinent to the law enforcement bodies and the general public, since it highlights a very important aspect of cybercrime and its far-reaching consequences on the digital landscape of India. The objective of the research is to assess and pinpoint the gaps that currently exist and put forward some concrete suggestions which in turn can foster a more secure cyber environment in the country. Cybercrime is omnipresent, impacting individuals, businesses, and the economy as a whole. Mobile banking, internet banking, social networking, and e-commerce, have more misuse, thus more types of cybercrime activities. The CERT-In Internet Crime Report of 2020 has shown that overall cybercrimes have expanded recently, more profoundly than even the gross domestic profit (GDP).

## 2. Legal Provisions for Cyber Crimes in India

### 2.1 The Information Technology Act, 2000

The IT Act of 2000 was India's first attempt to put some order over the issues in the realm of cybercrime and electronic commerce. It provides a basic framework for giving legal recognition to electronic transactions and digital signatures along with penalising cybercrimes. Notably, sections 65-75 of the IT Act deal with various cybercrimes like hacking, data theft, identity theft, cyberstalking and publishing obscene content.

### Relevant Sections of the IT Act

**Key sections of the IT Act include:**

**Section 66:** Punishment for hacking.

**Section 66C:** Identity theft.

**Section 66D:** infidelity by personation using computer

**Section 69A:** Power to block websites.

### 2.2 The Indian Penal Code, 1860 (IPC) and Cyber Crimes

provisions of the IPC. For example, in cases of data theft, the provisions of Section 378 (theft) and Section 403 (dishonest misappropriation of property) can be invoked and Section 507 (criminal intimidation), are applicable to cyber crimes. Section 500: Deals with defamation, applicable to cyber defamation cases.

### 2.3 Other Statutes Impacting Cyber Crimes

Besides the above two, some other laws dealing with cybercrimes in India are the Indian Evidence Act for collecting digital evidence; the Copyright Act, of 1957, concerning intellectual property; and the Bankers' Book Evidence Act of 1891, concerning all crimes related to online banking.

### 2.4 Data Protection Bill (currently in draft form):

Aimed at providing robust data protection and privacy safeguards.

## 3. Cyber Crimes in India

Causes and Impact of Cyber Crimes in India

### 3.1 Types of Cyber Crimes in India

**Hacking:** Hacking is one of the most common and destructive types of cybercrime. It involves unauthorized access to computer systems and networks to steal, alter, or destroy data. The Indian legal system penalizes playing under Section 66 of the IT Act.

**Identify Theft and Phishing:** Identity theft is the process of a person carrying information about another person to commit fraud. Phishing is a system used to gain sensitive information by pretending to be a trusted person. With the proliferation of the internet, fiscal deals over the internet have increased and the number of similar crimes has also increased.

**Cyberterrorism:** Cyberterrorism refers to the use of the Internet to beget serious detriment to public or public security. Section 66F of the Information Technologies Law defines cybercrime as

an act that harms the sovereignty, integrity and security of the country.

**Cyber Stalking and Harassment:** Cyberstalking and online importunity are becoming a problem, especially in times of gender-based violence. The Sequestration Act provides for penalties for transferring, draining or hanging emails.

**Fiscal Frauds and Cyber Fraud:** Cyber fraud, including phishing, credit card frauds, and online swindles, have become prevalent as people increasingly engage in online deals.

### 3.2 Causes of Cyber Crimes

**Technological Factors:** Increased internet penetration and lack of robust security measures.

**Social Factors:** Digital ignorance and over-reliance on technology.

**Profitable Factors:** The lure of financial gain and lack of employment openings.

### 3.3 Impact of Cyber Crimes on Society

#### 1) Profitable Impact

Cybercrime is causing millions of dollars in losses to businesses and individuals. The rise of ransomware and swindles has affected the country's GDP and business confidence. Billions of bones are lost to fraud and theft every time.

#### 2) Cerebral and Social Impact

The cerebral impact of bullying and importunity is particularly significant on women and children. Anxiety disorders are caused from cyberbullying, importunity, and libel. Cybercrime affects children and vulnerable groups in society.

#### 3) National Security and Sovereignty

Cybercrime and data breaches hang critical structure, system protection, and governance. Cybercrime and surveillance.

### 4. Challenges in Combating Cyber Crimes & Strategies to Mitigate Cyber Crimes

#### 4.1 Challenges in Combating Cyber Crimes

##### a) Technological Challenges

Rapid technological change creates challenges in developing laws that respond to cyber threats. It is also true that law enforcement lacks the expertise needed to conduct investigations. Law enforcement often faces challenges in investigating and prosecuting cybercrimes due to a lack of training and rapid response.

##### b) Lack of Digital Literacy and Lack of Awareness

Many people in rural India are unaware of cyber threats. This ignorance makes people vulnerable to cybercrimes such as online fraud and identity theft. Lack of knowledge about digital security is a major problem in the fight against cybercrime. Most people, including organizations, do not know how to keep their digital footprint safe, leaving them vulnerable to cyber thieves.

##### c) Data Privacy and Security Concerns

Additionally, the lack of legal data protection raises concerns about how data is stored, processed, and shared, opening the door to data breaches and cyberattacks.

##### d) Cross-Border Jurisdiction Issues

Cybercrime is committed by people from many other countries, both domestically and internationally. So, there is the issue of extradition, there is the issue of international cooperation and law enforcement. Cybercrime is mostly transnational. Since the perpetrators are committing crimes under foreign laws, it becomes difficult to punish them. India also does not have cybercrime cooperation agreements with some countries.

##### e) Inadequate Cyber law enforcement

The Information Technology Law and other laws are based on a lack of transparency and weak governance. Furthermore, the evolution of law has not kept pace with the development of new technologies.

### 4.2 Strategies to Mitigate Cyber Crimes

#### 1) Technological Measures

Uses advanced encryption techniques.

#### 2) Legal and Policy Reforms

Strengthening the IT Act with provisions for emerging crimes.

Establishing a national cyber security policy with actionable measures.

#### 3) Public Awareness and Education

Launching campaigns to educate citizens about online safety.

Integrating cyber security modules into school curricula.

#### 4) Capacity Building for Law Enforcement

Training programs for police and judiciary in handling cybercrime cases.

Establishing dedicated cybercrime cells in every district.

### 5. Landmark Case Laws in Cyber Crime in India

#### 5.1 Tamil Nadu State v. Suhas Katti (2004)

This case is one of the first to be ruled under Section 66A of the Information Technology Act. Suhas Katti is seen harassing the woman by sending her abusive and derogatory messages through emails and online forums. This is the first ruling under India's Information Technology Act. Suhas Katti was found guilty of sending obscene messages through emails and was arrested under Sections 66 and 67 of the Information Technology Act. This document was created to prosecute online obscenity and pornography under the Act.

#### 5.2 Cyber Appellate Tribunal Case (2004)

The case, which involved allegations of unauthorized access and tampering with personal data, eventually led to the establishment of the Cyber Appeals Court, which examines cases filed against individuals who commit cybercrimes and violate the Information Technologies Law.



### 5.3 TCS v. Anil Kumar (2006)

In this context, an employee of Tata Consultancy Services (TCS) steals sensitive information and becomes the real owner of the company's data theft database. This document has outlined the concept of data protection and the need for employers to secure their IT structures.

### 5.4 Dr. N. S. Kharbanda v. Union of India (2013)

The document addresses the government's responsibility to take stringent measures to protect cybersecurity and prevent cyber terrorism. The Delhi High Court stated that there is a need for greater collaboration between law enforcement agencies and technological solutions to combat cybercrime.

### 5.5 Shreya Singhal v. UOI (2015)

The evidence has struck down Section 66A of the IT Act, which criminalizes sending obscene messages through a communication service, social media platform, or website. The Supreme Court has ruled that these provisions are inappropriate as they violate Art.19(1) (a) of the Constitution of India. This information is important in the context of online freedom of expression and cybercrime. The SC of India has struck down Section 66A of the Information Technology Act, which makes sending obscene messages through a communication service or website illegal. The Bill has been found inappropriate as it is vague, broad in scope, and violates the right to freedom of expression.

### 5.6 Rajendra Mishra v. Union of India (2020)

The case involves internet fraud involving digital payments. The court ruled that banks and other financial institutions must improve their security procedures to protect against digital fraudsters and protect the financial information of their customers who become victims of fraud.

## CONCLUSION

Cybercrimes pose a significant threat to India's digital landscape. With the enactment of the IT Act, enforcement remains difficult due to technological gaps, lack of awareness, and jurisdictional issues. Case laws existing in India reflect an evolving legal approach towards cybercrime, as the judiciary has been stepping up to interpret progressive positions on issues such as free speech and privacy. Cybercrime in India is a critical challenge that needs a collaborative effort from all the public and private stakeholders. With a robust data-driven approach, this research endeavors to add to the understanding of cybercrime dynamics and propose practical solutions for enhancing India's cybersecurity resilience. It presents an area requiring urgent attention from all stakeholders regarding cybercrime in India. This Research is expected to deal exhaustively with the problem, appraise the measures already in place, and give recommendations for intervention to improve India's cybersecurity status. Cybercrime poses a risk to the entire Digital Economy and to Public Safety and National Security of India. However, several bottlenecks against effective enforcement remain, even as an overarching legal framework has evolved. In India, cyber crimes are

increasing in hours and breadth. However, both the issues of technology up-gradation, along with the police and public awareness challenge, they never entirely go away in the face of such governmental policies and measures. The answer requires a joint effort of the government, judiciary, law enforcement and public to surpass the same. Enhancing legal frameworks, promoting digital literacy, and boosting international collaboration are key to cultivating a safer cyber ecosystem in India. Cybercrimes are a bigger challenge in the digital ecosystem of India. The government makes efforts to battle these threats, but we need a multifaceted intervention in terms of the legal, technological, and social spaces. A collaborative spirit among stakeholders is going to be crucial for India in creating a safer cyberspace for everyone. A serious issue for the digital economy and security of India is the threat of cybercrimes. Effective mitigation will require a robust legal framework, technological progress, and public awareness.

**Table 1:** List of Cases

Sr. No.	Name of the Cases	Year
1.	Tamil Nadu State v. Suhas Katti	2004
2.	Cyber Appellate Tribunal Case	2004
3.	TCS v. Anil Kumar	2006
4.	Dr. N. S. Kharbanda v. UOI	2013
5.	Shreya Singhal v. UOI, 5 SCC 1	2015
6.	Rajendra Mishra v. UOI	2020

**Table 2:** List of Abbreviations

Abbreviation	Full Form
IT Act	Information Technology Act, 2000
HC	High Court
NCRB	National Crime Records Bureau
IPC	Indian Penal Code
IT	Information Technology
CERT-In	Indian Computer Emergency Response Team
SC	Supreme Court
GDP	Gross Domestic Product

## REFERENCES

1. Ministry of Electronics and Information Technology. Cybersecurity Initiatives in India [Internet]. Available from: <https://www.meity.gov.in>.
2. National Crime Records Bureau (NCRB). Annual Report on Cybercrime in India. 2022.
3. CERT-In. Annual Report on Cybersecurity Incidents [Internet]. 2022. Available from: <https://www.cert-in.org.in>.
4. Bhattacharya S, Ghosh I. Cybercrime in India: Trends and Implications. J Digit Secur. 2021;15(3):123-138.
5. Kshetri N. Cybersecurity in Emerging Economies: Challenges and Opportunities. Int J Inf Manag. 2020;50:102-112.
6. Sharma P. Legal Framework for Combating Cybercrime in India. Indian Law Rev. 2022;8(1):45-67.
7. Statista. Internet Usage in India: Statistics and Trends [Internet]. 2023. Available from: <https://www.statista.com>.
8. Bhasin M. Cyber Law and Information Security. New Delhi: McGraw Hill Education; 2018.

9. Singh Y. Cybercrime and Digital Forensics in India. Hyderabad: Pearson Education; 2020.
10. Law Commission of India. Report No. 267: Hate Speech and the Internet [Internet]. 2017. Available from: <https://lawcommissionofindia.nic.in>.
11. Law Commission of India. Report No. 156: Review of the Indian Penal Code [Internet]. 2000. Available from: <https://lawcommissionofindia.nic.in>.
12. Basu DD. Introduction to the Constitution of India. Gurgaon: LexisNexis India; 2019.
13. Ministry of Home Affairs. Cybercrime Prevention against Women and Children (CCPWC) Scheme [Internet]. 2021. Available from: <https://www.mha.gov.in>.
14. Digital India Programme. Promoting Cyber Hygiene and Cyber Awareness [Internet]. 2022. Available from: <https://www.digitalindia.gov.in>.
15. Information Security Education and Awareness (ISEA). Cybersecurity Training Initiatives [Internet]. 2022. Available from: <https://www.isea.gov.in>.
16. The Information Technology Act, 2000.
17. Indian Penal Code, 1860.
18. The Copyright Act, 1957.
19. Mittal S. Cybercrime Trends in India. Indian Law Rev. 2023;15:1-15.
20. Jain R. Analyzing the IT Act. J Cybersecur Law. 2022;1:1-10.
21. Criminal Law (Amendment) Act, 2013.
22. Shreya Singhal v. Union of India, 5 SCC 1 (2015).
23. State of Tamil Nadu v. Suhas Katti, 2004.
24. Rajendra Mishra v. Union of India, 2020.
25. TCS v. Anil Kumar, 2006.
26. Cyber Appellate Tribunal Case, 2004.
27. Dr. N. S. Kharbanda v. Union of India, 2013.
28. CERT-In. Cyber Crime Reports. 2020.
29. Parekh CS. Cyber Laws and Legal Issues in India. 2021.
30. Kshetri N. Digital Payment Systems and Cybersecurity in India. J Cyber Policy. 2019;1:1-12.
31. Bansal R, Arora M. The Role of Artificial Intelligence in Cyber Crime Prevention. Cybersecur J. 2021;5:100-110.
32. Gupta S, Malhotra P. Psychological Impact of Cyber Crimes on Victims. Indian J Cyber Psychol. 2023;1:1-10.
33. Sharma P, Verma S, Gupta R. Analyzing the Effectiveness of Cyber Laws in India. Int J Law Technol. 2022;1:45-67.
34. Verma A. Global Best Practices in Cyber Security: Lessons for India. Int J Cyber Secur Stud. 2023;2:1-20.

#### Creative Commons (CC) License

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license. This license permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.