Law Audience Journal, Volume 6 & Issue 1, 10th June 2025, e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.954, Published at https://www.lawaudience.com/volume-6-issue-1-2/, Pages: 80 to 92,

Title: Addressing Cybercrime in India: Challenges, Prosecution, and Prevention, ***Authored By: Rishabh Soni, LL.M. (Corporate Law), School of Law, Galgotias University, Greater Noida, U.P., Email Id: rishabhhsonii8@gmail.com.***

Cite this article as:

RISHABH SONI, *"Addressing Cybercrime in India: Challenges, Prosecution, and Prevention" Vol.6 & Issue 1, Law Audience Journal (e-ISSN: 2581-6705), Pages 80 to 92 (10th June 2025), available at https://www.lawaudience.com/a-comparative-study-on-emergency-provisions-of-british-india-and-present-day-sovereign-states/.*

Law Audience Journal, Volume 6 & Issue 1, 10th June 2025, e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.954, Published at https://www.lawaudience.com/volume-6-issue-1-2/, Pages: 80 to 92,

Title: Addressing Cybercrime in India: Challenges, Prosecution, and Prevention, Authored By: Rishabh Soni, LL.M. (Corporate Law), School of Law, Galgotias University, Greater Noida, U.P., Email Id: rishabhhsonii8@gmail.com.

Email(s): ***lawjournal@lawaudience.com, info@lawaudience.com, lawaudience@gmail.com.***
Phone (No(s)): ***+91-8351033361,***
Website: ***www.lawaudience.com.***
Facebook: ***www.facebook.com/lawaudience.***
Instagram: ***www.instagram.com/lawaudienceofficial.***
Contact Timings: ***10:00 AM to 8:00 PM.***

Law Audience Journal, Volume 6 & Issue 1, 10th June 2025, e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.954, Published at https://www.lawaudience.com/volume-6-issue-1-2/, Pages: 80 to 92,

Title: Addressing Cybercrime in India: Challenges, Prosecution, and Prevention, Authored By: Rishabh Soni, LL.M. (Corporate Law), School of Law, Galgotias University, Greater Noida, U.P., Email Id: rishabhhsonii8@gmail.com.

Disclaimer:

Law Audience Journal, Volume 6 & Issue 1, 10th June 2025, e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.954, Published at https://www.lawaudience.com/volume-6-issue-1-2/, Pages: 80 to 92,

Title: Addressing Cybercrime in India: Challenges, Prosecution, and Prevention, Authored By: Rishabh Soni, LL.M. (Corporate Law), School of Law, Galgotias University, Greater Noida, U.P., Email Id: rishabhhsonii8@gmail.com.

Publisher Details:

Law Audience Journal (e-ISSN: 2581-6705),

Sole Proprietorship of Mr. Varun Kumar, Kharar, District. S.A.S, Nagar, Mohali, 140301,

Phone No(s): +91-8351033361 (WhatsApp),

Email ID(s): lawjournal@lawaudience.com, info@lawaudience.com or lawaudience@gmail.com.

Website: www.lawaudience.com.

Contact Timings: 10:00 AM to 8:00 PM.

Editor(s):

Law Audience Journal, Volume 6 & Issue 1, 10th June 2025, e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.954, Published at https://www.lawaudience.com/volume-6-issue-1-2/, Pages: 80 to 92,

Title: Addressing Cybercrime in India: Challenges, Prosecution, and Prevention, Authored By: Rishabh Soni, LL.M. (Corporate Law), School of Law, Galgotias University, Greater Noida, U.P., Email Id: rishabhhsonii8@gmail.com.

ABSTRACT:

"Cybercrime has become a more significant problem in India due to the quick advancement in technologies connected with the extensive usage of the internet. For people, companies, and law enforcement organizations, the variety of cybercrimes, such as identity theft, financial fraud, cyberstalking, and data breaches, presents serious difficulties. Cybercrime prevention and punishment still confront several obstacles, even with the IT Act of 2000 and other provisions in the IPC. Confirmation in ***Sec 65B of the Indian Evidence Act****. The IT Act's safeguards from cybercrimes. Legal cases are complex; for instance, courts accept automation when it comes to the challenges for prosecutors of tying certain threshold requirements in the law to cybercrimes. One of the key issues is the collision between Article 21 of the Indian Constitution, giving us the right to privacy, and the argument that there is a major failing in the current legal structure. The matter is that when the matter comes about privacy as a human being, we need to understand nowadays every person is on social media using different types of platforms to show themselves, but under the limelight, they show something extra to society, which is not good for themselves. Significant enough, underlining the need for more holistic initiatives. It is often said that unawareness of cybersecurity initiatives makes us, the individual and the small business, an opportunity for hackers. While digital literacy campaigns and cybercrime units have been established, their reach and impact have not been wide or POV. The fundamental issue is that the public is ill-informed about digital threats to their safety, so from now on, the government should start some campaigns to teach about tech at different levels to ensure the safety of the people. A comprehensive approach is needed to address these issues, including enhancing enforcement mechanisms, strengthening legislative frameworks, making sure that rules related to the protection of intellectual property become clear, and promoting digital literacy. It is equally important to invest in innovative technologies, foster public-private partnerships, and improve cross-border collaboration. India must put strong policy measures in place to tackle cybercrime while finding a balance between people's rights and cybersecurity requirements The policies should be made for the betterment of society, as now the technology has gone*

Law Audience Journal, Volume 6 & Issue 1, 10th June 2025, e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.954, Published at https://www.lawaudience.com/volume-6-issue-1-2/, Pages: 80 to 92,

Title: Addressing Cybercrime in India: Challenges, Prosecution, and Prevention, Authored By: Rishabh Soni, LL.M. (Corporate Law), School of Law, Galgotias University, Greater Noida, U.P., Email Id: rishabhhsonii8@gmail.com.

farther and farther; it creates different types of innovation day by day, so the policies should be strict, and if any person tries to breach someone's privacy, they get strictly penalized. Countries should provide a safe and secure digital environment for their people and enterprises, and cooperation and openness are compulsory".

Keywords: Cybercrime, Right to Privacy, Information Technology Act, Digital Evidence, Prosecution Challenges, Prevention Strategies, Copyright Protection.

I. INTRODUCTION:

How people live, work, and communicate has been transformed by the ease of the digital age. There are many technological benefits, but it also has a dark side: the expansion of cybercrime, or the criminal activity that takes place on the internet. The risks from cybercrime are growing exponentially in India, where internet penetration has also been growing fast. Cybercrimes come in a range of forms, and several are scary, including identity theft and cyberbullying, as well as financial felonies and data breaches. And a real-court-sized system cannot handle these problems. Though there are existing laws like the Information Technology Act, 2000, and relevant sections in the Indian Penal Code (IPC), they all too often do not deliver justice in time or fail to act as a deterrent to a would-be wrongdoer, and given the complex nature of cybercrimes ***(often spread across various jurisdictions and often hiding behind advanced technology and anonymity),*** the challenge of prosecution and prevention becomes even more daunting. The issue is addressed by research. The central issue concerning the problem is the vast difference in the rate of increase of cybercrimes. Agencies are regularly doing their work to trace unlawful activity that happens anywhere and then can stop it. Cybercrimes are threatening not only the financial status and reputation of people and institutions but also endangering national security; therefore, combating such crimes is in great need for safeguarding the basic rights of the people, as well as the public trust in the digital economy. Also, understanding the

problems of the prosecution and deterrence of cybercrimes can help the legal community and government develop better policies and help bridge the divide between law and technology.

I.I OVERVIEW AND LEGISLATIVE CONTEXT:

This section will examine the increase of cybercrime in India and the resultant legislative attempts to regulate it, including key provisions of 66A of the Information Technology Act and other legislation.

(a) Prosecution Challenges: The current subsection will examine challenges such as the issue of jurisdiction, challenges to gather evidence, and the lack of technological skill amongst law enforcement agencies.

(b) Challenges in Prevention: The limitations of current legislation, the challenges of raising awareness, and the provision of cybersecurity infrastructure will be the primary focus of this portion.

I.II HYPOTHESIS:

Rapid technological advancements, legal framework gaps, and enforcement challenges have made cybercrime in India a growing concern. "To effectively combat and prevent cybercrime, even while existing laws and methods attempt to address this issue, there is an urgent need for stronger legal and technological infrastructure, increased awareness among those involved, and improved collaboration between law enforcement, government officials, and the private sector. From my point of view, we can handle these problems easily by educating people, organizing awareness campaigns, short video clips, caller tunes, double authentication processes, etc. These are some points by which we can help people save themselves from cyber fraud.

I.III RESEARCH OBJECTIVES:

Investigating the difficulties in crime prevention and prosecution in India, the study is to pinpoint the current legal and practical weaknesses and offer workable fixes to improve India's strategy against cybercrime.

The goals of this study are:

1. To assess India's present legal system for dealing with cybercrime:

An examination of the information technology-associated statutes, like the Indian Penal Code, is included in this.

2. To determine the difficulties in prosecuting cybercrimes:

   This means being aware of problems like a lack of technical skill, evidence collection difficulties, jurisdictional obstacles, and courtroom delays.

3. To investigate the existing preventive actions implemented to reduce cybercrime:

   A review of cybersecurity infrastructure, public awareness campaigns, and the function of law enforcement will all be part of this.

4. To evaluate how technological developments contribute to the prevention and assistance of cybercrime:

   The goal is to assess how hackers are utilizing emerging technologies and how cybersecurity measures can benefit from their utilization.

5. To provide suggestions for enhancing India's cybercrime prevention and prosecution systems:

   Public-private partnerships, interagency cooperation, capacity building, and legislative reforms will be the main focuses of this.

6. ComparingIndia'scybercrimestrategywithglobalbestpractices:

   This will give an outline of how other nations deal with comparable issues and what India may learn from them.

I.IV RESEARCH QUESTION:

I.IV.I PRIMARY RESEARCH QUESTION:

1. *Do India's current laws and regulations combat cybercrime, and what obstacles exist for their implementation and prosecution?*

I.IV.II SECONDARY RESEARCH QUESTIONS:

1. *To what extent do existing laws in India address the complexities of modern cybercrimes?*
2. *Does the current legal framework adequately protect the rights of victims of cybercrime in India?*

3. *Is the Indian judiciary equipped to handle the technicalities involved in cybercrime prosecution?*
4. *Does the interplay between Indian and international legal systems effectively combat transnational cybercrimes?*
5. *To what degree do gaps in investigation techniques hinder the successful prosecution of cybercrimes in India?*
6. *Is the enforcement of data protection and cybersecurity regulations sufficient to prevent cybercrime in India?*
7. *Do jurisdictional challenges pose a significant barrier to prosecuting cybercriminals operating across borders?*
8. *Are public awareness and digital literacy campaigns effective in reducing the occurrence of cybercrimes in India?*

I.V RESEARCH METHODOLOGY:

The focus of this study is doctrinal. As a way to answer the research issues, a doctrinal methodology examines current legislation, court rulings, and academic journals. Because it enables an in-depth study of statutes, case law, and academic literature to understand the legal framework and challenges linked to cybercrime prosecution and prevention in India, this approach is particularly appropriate for legal research.

I.V.I APPROACHES FOR GATHERING DATA:

I.V.I.I PRIMARY SOURCES:

Legal sources like these are the main source used in this study.

I.V.I.I.I STATUTORY LAWS:

The Information Technology Act of 2000 (as modified), the Indian Penal Code (IPC), and other relevant laws that control cybercrime in India.

I.V.I.I.II JUDICIAL DECISIONS:

To understand the judicial interpretation and implementation of cybercrime laws, read important case laws from India's Supreme Court and other high courts.

Law Audience Journal, Volume 6 & Issue 1, 10th June 2025, e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.954, Published at https://www.lawaudience.com/volume-6-issue-1-2/, Pages: 80 to 92,

Title: Addressing Cybercrime in India: Challenges, Prosecution, and Prevention, Authored By: Rishabh Soni, LL.M. (Corporate Law), School of Law, Galgotias University, Greater Noida, U.P., Email Id: rishabhhsonii8@gmail.com.

I.V.I.II SECONDARY SOURCE:

Books, research papers, reports, and commentary are among the materials used to learn more about the wider ramifications of cybercrime and the difficulties in preventing and prosecuting it.

Key secondary sources consist of

- *Academic journals and articles on cybercrime law and policy.*
- *Reports by organizations like the National Crime Records Bureau (NCRB) and other government bodies.*
- *Research studies by think tanks and international organizations address cybercrime trends and legal challenges.*

I.V.I.II.I LEGAL DATABASES:

- *For accurate and up-to-date legal references, databases like Manupatra and SCC Online were consulted. These sources helped me to locate relevant case laws and statutory provisions.*

I.V.I.III METHODS OF DATA ANALYSIS:

The collected data is analyzed qualitatively. The doctrinal approach focuses on critical evaluation and interpretation of:

I.V.I.III.I JUDICIAL PRECEDENTS:

To analyze the court's stance on key cybercrime cases and their effectiveness in interpreting and enforcing the laws.

I.V.I.III.II STATUTORY PROVISIONS:

To identify gaps in the law or areas that require reform or need to be updated.

II. UNDERSTANDING CYBERCRIME:

II.I DEFINITION AND SCOPE OF CYBERCRIME:

Cybercrime is the term for crimes carried out via computer networks, systems, or the internet against people, businesses, or governments. It involves using technology to carry out illegal

actions that could endanger people, property, or society. In India, cybercrimes are addressed under a statutory framework established by the ***Information Technology Act, 2000 ("IT Act")***. Any conduct involving deception, fraud, or improper use of computers or electronic communication devices is prohibited by Section 66 of IT conduct. Cybercrimes are defined by the ***"Budapest Convention"*** on Cybercrime as violations of computer data availability, confidentiality, and integrity. Although this agreement has not been formally ratified by the Indian legal system, its tenets are frequently applied as standards to understand cybercrimes.

II.II CYBERCRIME SCOPE:

As technology advances, cybercrime in India is becoming more and more common. Cybercrime includes a wide range of actions, such as, but not restricted to:

1. ***Hacking and Unauthorized Access:***

   The unlawful and harmful entry into computer networks or systems. Hacking is punishable under Section 66 of the IT Act.

2. ***Bluejacking And Recognition Thieving:***

   So basically, it showed how hackers can steal your private information by taking your private data by stalking your day-to-day activity; they are waiting for the moment you lose negligence, and they suddenly grab your details, including your bank account information, passwords, or Adhar number, etc., under the provisions of the IT Act, sections 66C and 66D.

3. ***Stalking Through Social Media and Harassment:***

   Stalkers usually use social media platforms to stalk somebody, like their Snapchat, Instagram & Facebook accounts, or other types of websites. They generate fake links to hack your device to spy on the person. Stalking comes under section 354D of the IPC.

4. ***Online Money Fraud:***

   Includes practices such as phishing emails, ATM cloning, and illegal online transactions that are intended to deceive people or businesses. Sections 420 of the IPC and 66C of the IT Act deal with these violations.

Law Audience Journal, Volume 6 & Issue 1, 10th June 2025, e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.954, Published at https://www.lawaudience.com/volume-6-issue-1-2/, Pages: 80 to 92,

Title: Addressing Cybercrime in India: Challenges, Prosecution, and Prevention, Authored By: Rishabh Soni, LL.M. (Corporate Law), School of Law, Galgotias University, Greater Noida, U.P., Email Id: rishabhhsonii8@gmail.com.

5. ***Cyberterrorism:***

The use of the internet to compromise public safety, vital infrastructure, or national security. The IT Act's Section 66 F specifically addresses cyber terrorism.

II.III TYPES OF CYBERCRIME:

Cybercrime refers to illegal activities conducted using computers, networks, or the internet. In India, the rise in technology usage has also led to an increase in cybercrimes. Below are the main types of cybercrimes:

1. **Hacking -** Hacking is an illegal entry into a computer system or network, usually with the intent of stealing confidential information or interfering with normal business operations. In India, it is a prevalent cybercrime that affects people, businesses, and government organizations. **For instance,** attacks to steal private information from banking organizations or government websites. Section 66 of the Information Technology Act of 2000 is a legal provision.
2. **Identity Theft -** To commit fraud or impersonation, this entails stealing someone's bank information, name, or Aadhaar number. **For example,** opening bank accounts or committing financial theft using credentials that have been stolen.
3. **Cyberstalking** includes repeatedly watching someone's online activity without their permission, sending threatening emails, and engaging in online harassment. **Example**: Using chat applications or social media to stalk someone.
4. **Phishing** is the practice of using phony emails, texts, or websites to fool people into divulging private information, such as bank account information or passwords. **Example**: Phishing emails asking for account verification that claim to be from a bank.
5. **Cyberterrorism**—The use of computers or the internet to launch attacks that threaten national security or interfere with critical systems is known as cyberterrorism. **For instance**, attacking electrical systems, disturbing financial markets, or distributing misleading data.
6. **Child pornography and online abuse:** This involves producing, disseminating, or

gaining access to obscene material featuring children. According to Indian law, such offenses are strictly forbidden and exploit youngsters.

7. **Statutory Citation:** Section 67B of the Information Technology Act of 2000, as well as the Protection of Children from Sexual Offenses (POCSO) Act of 2012.
8. **Defamation online**—publishing negative comments or anything about someone online that damages their reputation is known as online defamation. **For example**, making false allegations about someone on social media.

III. LITERATURE REVIEW:

Rapid technological development has resulted in cybercrime, which has grown to be a serious problem for legal and law enforcement systems everywhere, including India. With an emphasis on gaps and possible reforms, the literature review examines the current legal system, difficulties in prosecuting cybercrimes, and preventive methods to identify the problems and solve them.

IV. LEGAL FRAMEWORK IN INDIA: INDIA'S LEGAL SYSTEM:

In India, the Information Technology Act of 2000 represents the principal legislation about cybercrimes. In 2008, the amended IT Act was amended concerning identity theft (Section 66C), cyber terrorism (Section 66F), and pornography (Section 67A). However, several scholars argue that the IT Act simply does not keep pace with comprehensive provisions to address the nature of cybercrimes that are becoming immensely challenging. Appreciating the Act also depends heavily on judicial interpretations. For instance, in ***Shreya Singhal vs. Union of India (2015) 5 SCC 1***, the Supreme Court struck down Section 66A of the IT Act for infringing free speech provisions. They struck down the provision to protect the values of fundamental rights and to highlight the regulatory gaps concerning online abuse and online hate.

V. OBJECTION IN PROSECUTION:

- **Administration Issues:** Adequate execution of cybercrime is difficult when countries don't

cooperate, which is understandably a challenge because cybercriminals often operate in multiple countries. For example, cross-border data theft cases require countries to collaborate, which can be difficult.

- **Ostensibly, problems:** The tasks of gathering, preserving, and presenting digital evidence are always difficult. Section 65B of the Indian Evidence Act of 1872 was amended to include electronic evidence, but in ***Arjun Panditrao Khotkar vs. Kailas Kishanrao Gorantyal,*** (2020) 7 SCC 1, the Supreme Court insisted on strict adherence to the certification offered by Section 65B for electronic evidence, resulting in substantial practical difficulties for prosecution.

VI. DETERRING STEPS AGAINST CYBERCRIME IN INDIA:

India's rapidly growing tech sector has produced great innovations and, consequently, increased cybercrime. A strong preventive framework is necessary to adequately address this development ***(which poses a serious challenge).*** This section identifies four broad categories of measures that are important: the role of government and regulators, public awareness and education, international collaboration, and developing technologies**.**

VII. ROLE OF GOVERNMENT AND REGULATORY AUTHORITIES:

- ***Competency of cyber laws*:** In India, acts like the Information Technology Act, 2000, would be updated regularly because the nature of cybercrime consistently changes day by day, such as ransomware, deepfake, and voice clone fraud. Having looked at these unlawful activities, the legislation and the administration should consider making new laws or updating the old laws.
- ***Uphold the cybercrime units*:** In the now, there are dedicated units and cells, like the Cyber Crime Prevention against Women and Children (CCPWC) cell. The ability to counter and prevent cybercrime will be enhanced by having more of these units or

cells at the state and district levels.

- ***Partnership with the private sector:*** As we can see nowadays, the public sector allows the private sector to work with them, which helps to prevent online threats and fraud and boost the security of the network providers for better detection and prevention of cyber fraud.
- ***Public Awareness and Education:*** Programs like the Ministry of Home Affairs' ***"Cyber Swachhta Kendra"*** inform the public about common online risks, including malware and phishing. For a more expansive audience, these advertisements are intended to be carried out in regional languages.
- The workshops for the training have been conducted regularly because they help people to educate themselves about cybercrimes and be safe from these threats.

VIII. RECOMMENDATIONS:

1. ***Comprehensive Review of the IT Act, 2000:*** The main purpose of the IT Act of 2000 was to control electronic transactions and e-commerce. It has been modified throughout time to incorporate clauses that deal with cybercrimes. ***The Act does not yet, however, contain comprehensive rules on new dangers such as ransomware, phishing, and data breaches. A thorough analysis is required to:***

- Provide updated definitions for cybercrimes.
- Deal with jurisdictional issues related to international cybercrimes.
- Establish sanctions for repeat offenders.

2. ***Improving Mechanisms for Prosecution and Investigation:*** Cybercrime investigation calls for certain knowledge and certain equipment. The majority of Indian law enforcement organizations lack the necessary tools and training to deal with cybercrime. Among the recommendations are:

- Creating specialized cybercrime units in each state.
- Teaching cybersecurity and digital forensics to law enforcement officers.
- Establishing a centralized database to monitor and report cybercrimes.

1. **Implementing Strict Data Protection Regulations:** India does not have a strong data

protection system in place to secure sensitive and personal data. ***A thorough data protection law, like the planned Digital Personal Data Protection Act, 2023, can be enacted in the following ways:***

- *Defend users from illegal data breaches and identity theft.*
- *Companies should be required to maintain data security.*
- *Give victims of crimes involving data a legal redress.*

IX. CONCLUSION:

Although India's legal system has made outstanding progress in cybercrime, issues with prevention and prosecution still exist. Effective enforcement is challenged by jurisdictional concerns, insufficient infrastructure, and the growing sophistication of cyberattacks. Regulations such as the Information Technology Act of 2000 provide the foundation, but their application needs to be strengthened to handle new dangers. Furthermore, the judiciary and law enforcement agencies lack specific cybercrime training, which slows down justice and damages the system's credibility. Effective cross-border cybercrime prevention requires cooperation between the public, corporate, and international organizations. Digital literacy initiatives and public awareness campaigns are equally important for preventing cybercrime at the local level. In conclusion, India has to combat cybercrime completely through incorporating modern technologies, fortifying current regulatory frameworks, and encouraging stakeholder collaboration. Only by working together can the country face the challenges of prevention and punishment while guaranteeing a safer online environment for its citizens.

References:

Primary Source:

1. ***The Information Technology, 2000 (as amended in 2008)***

Relevant Sections:

Section 66: Computer-related offenses (hacking, identity theft).

Section 66A (now repealed): Misuse of electronic communication.

Section 66C: Identity theft.

Section 66D: Cheating by personation using computer resources.

Section 66F: Cyberterrorism.

Section 67: Obscenity and explicit content.

2. ***Indian Penal Code***

Relevant Sections:

Section 354D: Cyberstalking.

Section 420: Cheating and fraud, which is often linked to cybercrime. Section 499/500: Online defamation.

3. ***Judicial Decisions:***

ShreyaSinghal vs. UnionofIndia,(2015)5SCC1

LandmarkcaseinvalidatingSection66AoftheITAct.

ArjunPanditraoKhotkar vs.KailasKishanraoGorantyal,(2020)7SCC1

Puttaswamy v. Union of India, (2017) 10 SCC 1

4. ***Secondary Sources:***

BOOKS: Cyber Law in India by Vakul Sharma

The Law of Cyber Crimes and Information Technology Law" by S.R. Bhansali.

5. ***Reports:***

National Crime Records Bureau (NCRB)

Ministry of Home Affairs—Cyber Crime Coordination Centre.

6. ***Other Online Resources:***

Government Portals:

CyberCrimeReportingPortal (https://cybercrime.gov.in/)

Ministry of Electronics and Information Technology (MeitY).