INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

LEGAL CHALLENGES IN PROSECUTING CYBERCRIME UNDER THE INFORMATION TECHNOLOGY ACT, 2000

AUTHOR – ADITI SINGH* & MUDRA SINGH**

* STUDENT AT AMITY UNIVERSITY LUCKNOW

** ASSISTANT PROFESSOR AT AMITY UNIVERSITY LUCKNOW

BEST CITATION – ADITI SINGH & MUDRA SINGH, LEGAL CHALLENGES IN PROSECUTING CYBERCRIME UNDER THE INFORMATION TECHNOLOGY ACT, 2000, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (3) OF 2026, PG. 445-448, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/MPNN3001

ABSTRACT

The expansion of digital technologies and the rapid growth of internet accessibility in India have significantly contributed to the increase in cyber-related offences such as hacking, identity theft, cyber fraud, cyber terrorism, and online harassment. The Information Technology Act, 2000 serves as the primary legislation governing cyber offences in India and provides a legal framework for addressing crimes committed through digital means.

Despite the existence of this statutory framework, the prosecution of cybercrime continues to encounter several legal and procedural obstacles. These challenges include jurisdictional complexities, difficulties in establishing the admissibility of electronic evidence, limited technical expertise among investigative authorities, delays in investigation and trial, and inadequacies in the existing legislative provisions.

This research paper critically examines these challenges and highlights the need for stronger institutional mechanisms, updated legislation, and improved technological capabilities in order to enhance the effectiveness of cybercrime prosecution in India.
Keywords: Cybercrime, Information Technology Act 2000, Electronic Evidence, Jurisdiction, Cyber Law

Introduction

India's transition toward a digitally driven economy has substantially increased reliance on electronic communication, digital banking systems, online marketplaces, and e-governance services. Government initiatives such as Digital India have further accelerated internet penetration and technological adoption across both urban and rural regions of the country. While these developments have enhanced accessibility and efficiency, they have also created new opportunities for cybercriminal activities.

Crimes such as phishing attacks, identity theft, financial fraud, cyberstalking, ransomware attacks, and data breaches have become increasingly common in the digital environment. With technological advancement, cybercriminals are now utilizing sophisticated tools including encryption technologies, artificial intelligence, and cryptocurrency-based transactions to conceal their identity and avoid detection.

In response to these developments, the Information Technology Act, 2000 was enacted to provide legal recognition to electronic records and digital signatures while also introducing penalties for various cyber offences. The Act represents a significant milestone in the development of India's cyber law framework by establishing legal mechanisms for regulating

digital transactions and addressing computer-related crimes.

The provisions of the IT Act operate in conjunction with other important statutes such as the Indian Penal Code, Indian Evidence Act, and the Code of Criminal Procedure, which collectively form the legal basis for investigating and prosecuting cyber offences in India. However, despite the presence of this legislative framework, the effective prosecution of cybercrime remains challenging. Issues such as jurisdictional conflicts, difficulties in complying with evidentiary requirements under Section 65B of the Indian Evidence Act, lack of specialized technical knowledge among investigators, and complications arising from cross-border cyber offences continue to hinder enforcement. Additionally, the borderless nature of cyberspace often makes it difficult to identify offenders and secure digital evidence within a reasonable time frame. These challenges highlight the urgent need for legal reforms, institutional strengthening, and modernization of investigative processes to address cybercrime effectively.

Overview of Cyber Offences under the IT Act, 2000

The Information Technology Act criminalizes a variety of cyber offences and establishes penalties for unlawful activities involving computer systems and digital networks. Some of the key provisions include:

• Section 43 – unauthorized access to computer systems or networks and damage to digital data

• Section 66 – offences related to computer misuse and fraudulent activities

• Section 66C – identity theft involving misuse of passwords, digital signatures, or other identification features

• Section 66D – cheating by personation through electronic communication

• Section 66F – cyber terrorism threatening national security

• Section 67 – publication or transmission of obscene content through electronic platforms

The Information Technology (Amendment) Act, 2008 strengthened the legal framework by introducing provisions relating to data protection, cyber security, and national security concerns.

Legal Challenges in Prosecuting Cybercrime

Jurisdictional Issues

One of the major challenges in prosecuting cybercrime arises from jurisdictional complexities. Cyber offences frequently involve multiple geographical locations where the offender, victim, and data servers may all be situated in different countries. Although Section 75 of the IT Act provides for extraterritorial jurisdiction, effective enforcement often depends on cooperation between international law enforcement agencies. This dependence can lead to delays in investigation and procedural complications in obtaining evidence from foreign jurisdictions.

Admissibility of Electronic Evidence

The admissibility of electronic evidence is governed by Section 65B of the Indian Evidence Act, which requires proper certification for electronic records to be considered valid in court proceedings. Important judicial decisions such as Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) have emphasized strict compliance with these requirements. In practice, however, obtaining the required certification often proves difficult. Investigators may lack technical knowledge regarding digital evidence procedures, which can weaken the evidentiary value of electronic records and adversely affect prosecution.

Lack of Technical Expertise

The investigation of cyber offences requires specialized knowledge in areas such as digital forensics, cyber investigation techniques, and data analysis. Many law enforcement agencies lack sufficient training and technological infrastructure to effectively handle such cases. As a result, evidence may be improperly collected, preserved, or analyzed, ultimately weakening the prosecution's case.

Delay in Investigation and Trial

Another major obstacle in cybercrime

prosecution is the delay in investigation and judicial proceedings. Cyber forensic laboratories in India often experience significant backlogs due to limited resources and a high volume of cases. Additionally, international cooperation requests and data retrieval from foreign service providers can further prolong investigations.

Anonymity and Encryption

Modern technologies allow cybercriminals to conceal their identities through the use of Virtual Private Networks (VPNs), encrypted messaging platforms, and dark web networks. These tools make it extremely difficult for investigators to trace the individuals responsible for cyber offences. Furthermore, authorities must carefully balance investigative powers with the right to privacy under Article 21 of the Constitution, making regulation and enforcement more complex.

Outdated Legislative Framework

The rapid evolution of digital technologies has created new forms of cybercrime that are not fully addressed by the existing provisions of the IT Act. Emerging threats include:

- Cryptocurrency-based financial fraud
- Artificial intelligence-driven scams
- Deepfake technology used for misinformation and identity manipulation

These developments demonstrate the need for periodic updates to cyber legislation in order to address emerging technological threats effectively.

Landmark Judicial Interpretations

Judicial decisions have played a crucial role in shaping India's cyber law framework. In Shreya Singhal v. Union of India (2015), the Supreme Court declared Section 66A of the IT Act unconstitutional on the grounds that it violated the fundamental right to freedom of speech and expression. While this judgment strengthened constitutional protections, it also created certain challenges in regulating online harassment and offensive communication. Another notable case is State of Tamil Nadu v. Suhas Katti (2004), which is considered one of the earliest successful convictions under the IT Act for cyber harassment.

Suggestions and Reforms

To strengthen the prosecution of cyber offences in India, several measures can be adopted:

1. Establishment of specialized cybercrime courts to handle digital offences efficiently.
2. Development of advanced digital forensic laboratories and infrastructure.
3. Provision of regular technical training programs for police officers, investigators, and prosecutors.
4. Simplification of procedures related to the admissibility of electronic evidence.
5. Continuous updating of cyber laws to address emerging technologies such as artificial intelligence, cryptocurrency, and deepfake media.

Conclusion

The Information Technology Act, 2000 forms the backbone of India's legal framework for addressing cyber offences. However, the prosecution of cybercrime continues to face numerous challenges including jurisdictional issues, evidentiary difficulties, procedural delays, and rapidly evolving technological threats.

To effectively combat cybercrime, India must strengthen its legal and institutional mechanisms by updating legislation, improving technological infrastructure, and enhancing the capacity of law enforcement agencies. Such reforms are essential for ensuring a secure and reliable digital environment in the modern era.

References

1. Information Technology Act, 2000 (as amended in 2008).
2. Indian Penal Code, 1860.
3. Indian Evidence Act, 1872.
4. Code of Criminal Procedure, 1973.
5. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
6. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
7. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
8. State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004.
9. Aparna Viswanathan, Cyber Law in India

(LexisNexis).
10. Pavan Duggal, Cyber Law: The Indian Perspective.