CYBER CRIME AND INFORMATION TECHNOLOGY ACT 2000 IN INDIA: A CRITICAL LEGAL ANALYSIS

by

S. Naveen
S.Thangapazham Law College, Tamilnadu.

&

K.RAJESH KUMAR, (Ph.D)
Faculty of Law, S.Thangapazham Law College, Tamilnadu.

ABSTRACT

The rapid expansion of computers, smartphones, digital payments, social media and online services has created new opportunities for communication and commerce, but it has also generated new forms of unlawful conduct. Cyber crime includes offences committed through or against computers, networks and digital information. In India, the Information Technology Act, 2000 (IT Act) is the principal special legislation dealing with electronic records, electronic signatures, computer-related offences and several forms of cyber misconduct. The Act was substantially strengthened by the Information Technology (Amendment) Act, 2008. This research examines the concept and types of cyber crime, the statutory provisions of the IT Act, important judicial decisions, procedural and evidentiary issues, and the challenges faced by law-enforcement agencies. Particular attention is given to Shreya Singhal v. Union of India, Anvar P.V. v. P.K. Basheer, Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, and State of Tamil Nadu v. Suhas Katti. The paper concludes that effective cyber-crime control requires not only legislation but also digital forensic capacity, trained investigators, international cooperation, privacy safeguards and public awareness.

Keywords: Cyber Crime; Information Technology Act, 2000; Electronic Evidence; Cyber Security; Digital Forensics; Section 66; Section 67; Section 69A.

1. INTRODUCTION

The digital transformation of Indian society has changed the manner in which individuals communicate, conduct business, and make payments, store information and access public services. The same technological environment, however, may be exploited for unlawful purposes. Cyber crime is therefore a major legal and social challenge because the offender can operate remotely,

conceal identity, manipulate digital evidence and target victims across territorial boundaries. Unlike many conventional offences, a cyber offence may be committed in one jurisdiction, affect a victim in another and involve digital infrastructure located in several countries.

India enacted the Information Technology Act, 2000 to provide legal recognition to electronic records and electronic commerce and to facilitate electronic filing with government agencies.[1] The legislation also created a framework for dealing with specified offences involving computers and computer resources. The Information Technology (Amendment) Act, 2008 expanded this framework and introduced, among other provisions, offences concerning identity theft, cheating by personation through computer resources, violation of privacy, cyber terrorism and certain forms of obscene or sexually explicit electronic content.[2] The scale of this challenge has grown considerably in the years since the 2008 amendment. According to the National Crime Records Bureau, cybercrime cases registered across India rose by 31.2 per cent in a single year, from 65,893 cases in 2022 to 86,420 cases in 2023, with online fraud accounting for the largest share of these offences. This sustained increase illustrates why the statutory framework created by the IT Act continues to be tested with growing frequency by investigating agencies and the courts. *National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, 2025).*

.2. MEANING AND NATURE OF CYBER CRIME

The expression “cyber crime” does not have one universally accepted statutory definition. Broadly, it refers to unlawful acts in which a computer, computer system, computer network, communication device or digital data is the target, tool or environment of the offence. Cyber crime can therefore include attacks on computer systems as well as traditional offences committed through digital technologies.

Cyber crime has distinctive characteristics. It is often borderless, technically complex, capable of being committed at high speed and capable of causing extensive harm through a single digital act. Digital evidence may also be volatile: logs can be deleted, accounts can be altered and data can be encrypted or stored outside India. Consequently, investigation requires technical expertise and legally sound procedures for collection, preservation and presentation of electronic evidence.

The cross-border character of cyber crime is compounded by the slow pace of international evidentiary cooperation. A Council of Europe assessment of India's engagement with the Budapest Convention on Cybercrime found that responses to mutual legal assistance requests in cybercrime matters typically take between six and twenty-four months, a delay that often results in the loss or unavailability of volatile digital evidence by the time cooperation is secured. This gap between the speed of cyber offending and the pace of formal international cooperation is frequently identified as one of the most significant practical obstacles to effective investigation. *Cybercrime Convention*

---

1. *Information Technology Act, 2000, Statement of Objects and Reasons.*
2. *Information Technology (Amendment) Act, 2008 (Act 10 of 2009), provisions inserting and amending, inter alia, ss. 66A–66F, 67A–67C, 69A, 70B and related provisions*

Committee, 'India and the Budapest Convention: Why Not?' (Council of Europe, 10 August 2016) accessed 13 August 2026.

3. MAJOR TYPES OF CYBER CRIME

Common forms include unauthorised access or hacking, data theft, malware and ransomware attacks, phishing, online identity theft, cyber stalking, cyber harassment, cheating by online personation, publication or transmission of prohibited electronic content, attacks on critical information infrastructure and cyber terrorism. Financial cyber fraud has become especially significant because online banking, payment applications and digital commerce provide opportunities for criminals to deceive victims and rapidly transfer illicit proceeds. The financial scale of this trend is considerable. Data from the Indian Cyber Crime Coordination Centre indicate that victims in India lost approximately Rs 11,333 crore to cyber fraud in the first nine months of 2024 alone, with stock-trading and investment scams accounting for the largest share of these losses. Newer variants such as so-called 'digital arrest' fraud, in which victims are deceived into believing they are under investigation by a law-enforcement agency, have also emerged as a rapidly growing category of financial cybercrime. *'India Lost Rs 11,333 Crore to Cyber Fraud in 2024: Report' The Wire (New Delhi, 28 November 2024) accessed 13 August 2026.*

4. OBJECTIVES OF THE RESEARCH

The principal objectives of this study are to examine the legal meaning and forms of cyber crime; analyse the relevant provisions of the IT Act, 2000; understand the approach of Indian courts to cyber offences and electronic evidence; identify practical difficulties in investigation and prosecution; and suggest measures for strengthening the Indian cyber-law framework.

5. LEGAL FRAMEWORK UNDER THE INFORMATION TECHNOLOGY ACT, 2000

The IT Act, 2000 provides legal recognition to electronic records and electronic signatures and establishes a statutory framework for electronic governance.[3] Its criminal provisions are particularly important in responding to cyber offences. The Act operates alongside the general criminal law and other special legislation; therefore, conduct committed through a computer may attract provisions of the IT Act as well as provisions of the Bharatiya Nyaya Sanhita, 2023, depending on the facts of the case.

3. Information Technology Act, 2000

5.1 Section 43 – Unauthorised Acts and Compensation

Section 43 provides for liability where a person, without permission of the owner or person in charge of a computer, computer system or computer network, commits specified acts such as unauthorised access, downloading or copying data, introducing a computer contaminant or causing damage. The provision primarily provides a compensation-based remedy. Where the conduct is done dishonestly or fraudulently, Section 66 may convert the relevant conduct into a criminal offence.[4] In practice, however, the civil remedy under Section 43 remains considerably less used than the criminal route, with victims and investigating agencies more commonly pursuing prosecution under Section 66 or ordinary criminal law rather than approaching the adjudicating officer for compensation. Commentators attribute this partly to limited public awareness of the adjudicatory mechanism and to inconsistent capacity across states to process such claims, suggesting that greater use of this compensatory route could reduce pressure on the criminal justice system for lower-value disputes. *S Elavarasi and NP Elango, 'Analysis of Cybercrime Investigation Mechanism in India' (2020) 13 Indian Journal of Science and Technology 1 accessed 13 August 2026.*

5.2 Section 65 – Tampering with Computer Source Documents

Section 65 criminalises knowingly or intentionally concealing, destroying or altering computer source code required by law to be maintained. The provision recognises that manipulation of source code can compromise the integrity and reliability of computer systems.

5.3 Section 66 – Computer-Related Offences

Section 66 provides criminal punishment where any act referred to in Section 43 is done dishonestly or fraudulently. It is therefore an important provision for prosecuting several forms of unauthorised access, data interference and computer misuse. The statutory requirement of dishonest or fraudulent intention is important when determining criminal liability.

5.4 Sections 66C and 66D – Identity Theft and Online Personation

Section 66C addresses identity theft, including fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature. Section 66D deals with cheating by personation using a communication device or computer resource. These provisions are particularly relevant to phishing, fake profiles, fraudulent messages and online banking scams. The scale of such personation-based fraud has grown sharply in recent years. Data collated from national cybercrime records indicate that complaints of cheating by personation nearly doubled between 2022 and 2023, while incidents of banking and one-time-password related fraud have increased several-fold since 2018, reflecting the growing sophistication of phishing campaigns targeting digital payment users. This trend underlines the practical importance of Sections 66C and 66D in prosecuting the identity-based fraud that now forms a substantial share of reported cybercrime in India. *'Cybercrimes Up 217% in the Past Five Years: Insights from the NCRB Report' (Safer Internet India, 2025) accessed 13 August 2026.*

5.5 Section 66E – Violation of Privacy

Section 66E punishes intentional or knowing capture, publication or transmission of an image of a private area of a person without consent, under circumstances violating that person's privacy. The provision reflects the need to protect personal dignity and privacy in the digital environment.

5.6 Section 66F – Cyber Terrorism

Section 66F deals with cyber terrorism. It covers serious conduct involving computer resources where the statutory requirements relating to threats to the security, sovereignty or integrity of India, defence, security, critical infrastructure or other protected interests are satisfied. The provision demonstrates that cyber law is also connected with national security.

6. OTHER IMPORTANT PROVISIONS

6.1 Sections 67, 67A and 67B – Objectionable Electronic Content

Section 67 concerns publishing or transmitting obscene material in electronic form. Section 67A addresses material containing sexually explicit acts or conduct, while Section 67B specifically concerns material depicting children in sexually explicit conduct and related activities. These provisions seek to prevent misuse of digital platforms for dissemination of prohibited content while operating within constitutional limitations and procedural safeguards. The scale of the underlying problem is significant. Figures shared by the National Human Rights Commission indicate that India accounted for over five million of the roughly thirty-two million global tip-line reports of child sexual abuse material received in a single year by the United States-based National Center for Missing and Exploited Children, with reported domestic cases rising sharply between 2021 and 2023. This has prompted calls, including from the Commission itself, for a clearer statutory definition of 'sexually explicit' material under Section 67B to improve detection and removal of such content. *'NHRC Issues Advisory on Child Sex Abuse Material' Deccan Herald (Bengaluru, 2023) accessed 13 August 2026.*

6.2 Section 69A – Blocking of Information

Section 69A authorises the Central Government, or an authorised officer, to issue directions for blocking public access to information through a computer resource when the statutory grounds are satisfied and the prescribed procedure is followed.[5] The provision has constitutional significance because restrictions affecting online speech must be consistent with Article 19(2) and the safeguards recognised by law. The exercise of this blocking power has expanded considerably in recent years, with the government reportedly directing the restriction of over 36,800 accounts, websites and URLs between 2018 and 2023, including 7,502 in 2023 alone. Press-freedom monitors have repeatedly noted that the blocking process under Section 69A affords limited opportunity for affected persons or platforms to be heard before an order takes effect, raising continuing concerns about procedural transparency even where the underlying statutory objective is legitimate. *Freedom House, Freedom on the Net 2024: India (Freedom House, 2024) accessed 13 August 2026.*

---

4. Information Technology Act, 2000, § 43, relating to penalty and compensation for damage to computer, computer system or computer network, as amended from time to time.

6.3 Section 70 – Protected Systems

Section 70 permits the appropriate government to declare a computer resource affecting Critical Information Infrastructure as a protected system. Unauthorised access to or attempt to secure access to such protected systems is punishable. Protection of critical digital infrastructure is essential because disruption of sectors such as banking, telecommunications, energy or public services may produce consequences beyond individual victims.

6.4 Section 70B – CERT-In

Section 70B recognises the Indian Computer Emergency Response Team (CERT-In) as the national agency for performing functions relating to cyber security incidents. CERT-In has an important role in collecting and analysing information about cyber incidents, issuing alerts and advisories, coordinating responses and providing guidelines concerning cyber security practices. The volume of incidents handled by CERT-In has increased substantially over time. Government data placed before Parliament recorded a rise from roughly 394,000 cyber security incidents in 2019 to nearly 1.6 million incidents in 2023, with incidents affecting government organisations alone rising from about 85,800 to over 204,800 during the same period. This trajectory underscores the growing operational demands placed on CERT-In as the nodal agency for cyber incident response in India. *'India's Cybersecurity Incidents Hit 1.59 Million in 2023: CERT-In' (APAC News Network, 7 December 2024) accessed 13 August 2026.*

6.5 Section 72 and Section 72A – Confidentiality and Privacy

Section 72 provides punishment for breach of confidentiality and privacy in circumstances covered by the Act. Section 72A addresses disclosure of information in breach of lawful contract. These provisions are relevant to the protection of information obtained in the course of lawful access to digital systems and services.

5. Id., s. 69A; Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

7. PROCEDURAL AND EVIDENTIARY DIMENSIONS

Cyber-crime prosecution depends heavily upon electronic evidence such as emails, server logs, call records, metadata, CCTV footage, device images and social-media records. The Bharatiya Sakshya Adhiniyam, 2023 now governs evidence in India and contains provisions specifically addressing electronic or digital records.[6] The evidentiary process must establish authenticity, integrity, relevance and a reliable chain of custody. Investigators should document seizure, imaging, hashing, storage and examination of digital devices and records so that the evidence can withstand judicial scrutiny. These procedural demands are made more difficult by a persistent shortage of trained forensic personnel. Commentators have observed that many state forensic laboratories face acute shortages of qualified digital forensic examiners, with high attrition to better-paid private sector roles, even as the volume of digital evidence submitted for examination continues to rise. This capacity gap is reflected in enforcement outcomes: one analysis noted that only around 22.6 per cent of cybercrime cases registered in Bengaluru in 2022 resulted in a chargesheet, illustrating how forensic and investigative bottlenecks can undermine the practical effectiveness of the statutory framework. *'India's Cyber Forensics Push Since 2020: Building National Capacity for Digital Investigations' (Observer Research Foundation, 24 June 2025) accessed 13 August 2026.*

8. IMPORTANT CASE LAWS

8.1 Shreya Singhal v. Union of India

In Shreya Singhal v. Union of India,[7] the Supreme Court examined Section 66A of the IT Act, which criminalised sending certain information through a communication service. The Court struck down Section 66A as unconstitutional on the ground that it did not fall within the permissible restrictions on freedom of speech under Article 19(2). The decision is a landmark authority demonstrating that cyber regulation must conform to constitutional guarantees and that vague or overbroad restrictions on online speech cannot be sustained. Notably, however, empirical tracking by digital rights researchers has shown that Section 66A continued to be invoked by police and lower courts for several years after it was struck down, with data collated from a sample of states indicating that several hundred fresh cases were registered under the provision even after 2015. This gap between the constitutional pronouncement in Shreya Singhal and its practical implementation illustrates that striking down a provision does not, by itself, guarantee its disappearance from day-to-day policing, and points to the need for more systematic mechanisms for communicating judicial rulings to subordinate authorities. *'Recalling Why Section 66A of IT Act Was Struck Down' The Leaflet (6 November 2024) accessed 13 August 2026.*

8.2 Anvar P.V. v. P.K. Basheer

In Anvar P.V. v. P.K. Basheer,[8] the Supreme Court clarified the law concerning electronic records under the Indian Evidence Act, particularly the requirement associated with Section 65B. The judgment emphasised the statutory conditions governing admissibility of electronic records and became a leading authority on electronic evidence.

8.3 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal

In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,[9] the Supreme Court reaffirmed and explained the principles relating to Section 65B of the Indian Evidence Act and electronic evidence, while clarifying the relationship between primary electronic evidence and the statutory certificate requirement. The judgment remains important for understanding how courts approach authenticity and admissibility of digital material, subject to the current evidentiary framework under the Bharatiya Sakshya Adhiniyam, 2023.

State of Tamil Nadu v. Suhas Katti

State of Tamil Nadu v. Suhas Katti, decided by the Chief Metropolitan Magistrate, Egmore, Chennai, on 5 November 2004, is widely regarded as India's first conviction secured under the Information Technology Act, 2000. The accused was convicted under Section 67 of the Act, together with related provisions of the Indian Penal Code, for posting obscene and defamatory messages about the complainant in an online messaging group, and the case is frequently cited for having reached conviction within a relatively short period of the complaint being filed and for its early reliance on electronic evidence. The decision remains significant less for any point of statutory interpretation than for demonstrating, at an early stage in the life of the IT Act, that electronic communications could form the basis of a successful criminal prosecution. *'Case Summary: State of Tamil Nadu Vs Suhas Katti - Cyber Law Case in India' (E-Justice India, 2020) accessed 13 August 2026.*

9. CHALLENGES IN CONTROLLING CYBER CRIME

The first major challenge is jurisdiction. Cyber offenders can operate from outside the victim's country, making investigation dependent on international cooperation and timely access to foreign-held data. Mutual legal assistance procedures can be slower than the speed at which digital evidence disappears. Effective investigation therefore requires international cooperation, specialised protocols and cooperation with service providers within the limits of law. India's position outside the Budapest Convention on Cybercrime, the only binding multilateral treaty specifically addressing cross-border cyber offences and evidence-sharing, has been cited by commentators as one structural reason for the comparatively slow pace of international cooperation available to Indian investigators. While India continues to rely on bilateral mutual legal assistance arrangements, participation in a wider multilateral framework could, according to some analyses, streamline the preservation and exchange of volatile electronic evidence held abroad. *'Budapest Convention and the Information Technology Act' (Centre for Internet and Society, 2013) accessed 13 August 2026.*

---

6. BharatiyaSakshyaAdhiniyam, 2023, provisions relating to electronic or digital records and admissibility thereof.
7. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

The second challenge is technical complexity. Modern attacks may involve encryption, anonymisation tools, cryptocurrency, botnets, artificial intelligence and sophisticated malware. Police officers and prosecutors require continuing training in digital forensics, network security, mobile-device examination and financial tracing. Courts also require clear and reliable expert evidence to evaluate technical claims. The emergence of so-called 'digital arrest' scams illustrates the scale of this technical and social-engineering challenge. Government data placed before Parliament indicated that reported losses from such scams rose sharply through 2023 and 2024, with fraudsters impersonating law-enforcement or investigative agencies to coerce victims, before coordinated countermeasures such as account-freezing and public awareness campaigns contributed to a decline in reported cases in 2025. Such schemes demonstrate how rapidly criminal methods can evolve to exploit both technology and public unfamiliarity with legal process. *'After 465% Spike in 2024, MHA Data Shows Digital Arrest Scams Are on a Decline in India' ThePrint (18 February 2026) accessed 13 August 2026.*

The third challenge concerns electronic evidence. Digital evidence can be altered, copied or deleted without obvious physical traces. Poor seizure procedures, incomplete documentation or failure to preserve metadata may weaken a prosecution. A robust chain of custody and forensic methodology are therefore essential.

The fourth challenge is balancing cyber security with privacy and freedom of speech
Government agencies must have adequate powers to prevent serious cyber threats, but those powers must be exercised according to law and constitutional safeguards. The Supreme Court's decision in Shreya Singhal illustrates the constitutional limits applicable to online regulation.

10. CONCLUSION

Cyber crime represents one of the most rapidly evolving areas of modern criminal law. The expansion of digital services has increased the benefits of technology but has simultaneously created opportunities for unauthorised access, identity theft, online cheating, privacy violations, prohibited content and attacks against critical infrastructure. The Information Technology Act, 2000, as amended in 2008, provides an essential statutory framework for addressing many of these threats.

The effectiveness of cyber-crime law, however, depends on more than the existence of offences and penalties. Successful prosecution requires technically competent investigation, reliable digital forensics, proper preservation of electronic evidence, trained prosecutors and effective judicial understanding of technology. At the same time, cyber regulation must respect fundamental rights, particularly privacy and freedom of speech. The Supreme Court's jurisprudence demonstrates that technological regulation remains subject to constitutional review.

A comprehensive approach should therefore combine legislation, institutional capacity, cyber-security education, international cooperation and responsible technological practices. As new forms of cyber crime emerge through artificial intelligence, deepfakes, ransomware and increasingly sophisticated digital fraud, India's legal and institutional framework must remain adaptive. The ultimate objective should be to create a digital environment that protects individuals, businesses and

State while preserving constitutional freedoms and the legitimate benefits of technological development.

Sustaining such a comprehensive approach requires consistent institutional investment. Recent budgetary analysis has noted that allocations for cyber-security capacity, including for the Data Protection Board and related digital-forensics infrastructure, have grown only marginally relative to the scale of reported losses from cyber fraud, suggesting that funding commitments will need to keep pace with the rapidly expanding threat if institutional capacity is to remain adequate. *'Digital Arrest Scams and the Limits of Domestic Enforcement' (Observer Research Foundation, 2026) accessed 13 August 2026.*

REFERENCES

1. Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act, 2008.
2. Bharatiya Sakshya Adhiniyam, 2023.
3. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
4. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
5. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
6. Avnish Bajaj v. State (NCT of Delhi), 150 (2008) DLT 769.
7. State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004.
8. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
9. Indian Computer Emergency Response Team (CERT-In), official advisories and directions on cyber security incidents.
10. Ministry of Electronics and Information Technology, Government of India, official materials on the Information Technology Act and cyber security.

BIBLIOGRAPHY

1. Vakul Sharma, Information Technology law and practice, Universal Law Publishing
2. R.K.Bangia, Cyber Law, Allahabad Law
3. Pavan Duggal, Cyber Law, Universal Law