

International Journal Research Publication Analysis

Page: 01-08

CYBER CRIME IN INDIA: LEGAL FRAMEWORK, CHALLENGES AND REFORMS AN ACADEMIC RESEARCH ARTICLE

***Thakur Gulshan Kumar Amarnath**

B wing 206, Madhav Residency Dandiwad Faliya Balitha Vapi.

Article Received: 17 September 2026

*Corresponding Author: Thakur Gulshan Kumar Amarnath

Article Revised: 07 October 2026

B wing 206, Madhav Residency Dandiwad Faliya Balitha Vapi.

Published on: 27 October 2026

DOI: <https://doi-doi.org/101555/ijrpa.8942>

ABSTRACT

India's rapid digital transformation has expanded access to banking, education, commerce, communication and public services. At the same time, it has created opportunities for cybercrime, including phishing, online financial fraud, identity theft, unauthorised access, cyberstalking, ransomware, data theft and the circulation of unlawful digital content. Cybercrime is difficult to investigate because offenders may conceal their identities, act across borders, use rapidly changing technologies and store evidence in multiple jurisdictions. India's legal response is based principally on the Information Technology Act, 2000, read where applicable with general criminal law, evidence law, data-protection law and sector-specific regulation. The Bharatiya Nyaya Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023 form part of the contemporary criminal-law and evidence framework. Institutional mechanisms such as CERT-In, the Indian Cyber Crime Coordination Centre and the National Cyber Crime Reporting Portal support prevention, reporting and investigation. This article analyses the nature of cybercrime, the relevant legal framework, constitutional and evidentiary issues, enforcement challenges and reforms needed to improve victim protection and accountability. It argues that effective cybercrime control requires coordinated enforcement, technically competent investigation, reliable electronic evidence, public awareness and safeguards for privacy and civil liberties.

1. INTRODUCTION

Digital technology now plays a central role in daily life. Individuals use mobile phones and online platforms to make payments, communicate, study, work and access government services. Businesses depend on digital systems to store customer information and conduct

transactions. This growth has created substantial social and economic benefits, but it has also increased exposure to technology-enabled crime.

Cybercrime may target a computer, network or digital account, or use technology as a means of committing an offence. A fraudster may impersonate a bank employee to obtain a one-time password; a criminal may steal personal information to take over an account; or an attacker may encrypt an organisation's files and demand payment. Some offences are committed entirely online, while others involve a digital element within a conventional crime.

Cybercrime presents special enforcement problems. The person using an account may not be the account holder, electronic records can be deleted or altered, and data may be held by service providers in other countries. Investigators must therefore combine legal knowledge with digital forensics, timely preservation of records and cooperation among police, banks, telecommunications providers and technology companies.

2. SCOPE AND OBJECTIVES

This article examines major forms of cybercrime in India, the principal statutory framework, electronic evidence, enforcement institutions and the reforms needed to improve prevention and prosecution. Its objectives are to: (i) explain the meaning and characteristics of cybercrime; (ii) identify common cyber offences; (iii) analyse the relevant laws; (iv) discuss reporting, investigation and evidentiary issues; and (v) recommend practical legal and institutional reforms.

3. KEYWORDS: Cybercrime; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; Cybersecurity; Digital Evidence; Privacy; Online Fraud; CERT-In; Cyber Law.

4. MEANING AND NATURE OF CYBERCRIME

Cybercrime is a broad term for unlawful conduct involving computers, communication networks, digital data or online services. It can be divided into three overlapping categories: crimes against computer systems, such as unauthorised access or disruption; crimes committed through digital systems, such as online cheating and identity fraud; and offences involving unlawful digital content, including certain forms of sexually explicit material and abuse.

The defining features of cybercrime include speed, anonymity, scale, cross-border reach and dependence on electronic evidence. A single fraudulent message may reach thousands of people, and an offender may use false identities, virtual private networks, compromised

devices or money-mule accounts. These features complicate attribution and make early reporting particularly important.

5. MAJOR FORMS OF CYBERCRIME IN INDIA

5.1 Phishing and online financial fraud

Phishing involves deceptive messages or websites designed to obtain passwords, banking details or other confidential information. Related scams include fake customer-care numbers, investment fraud, QR-code deception, impersonation calls and fraudulent payment requests. Victims should immediately contact their bank or payment provider and report financial cyber fraud through the official helpline 1930 and the National Cyber Crime Reporting Portal.

5.2 Identity theft and impersonation

Criminals may misuse identity documents, passwords, SIM cards or digital credentials to impersonate another person. Identity theft can lead to financial loss, fraudulent accounts, reputational damage and unauthorised access to services. Section 66C of the Information Technology Act addresses identity theft involving specified electronic signatures, passwords or unique identification features, while Section 66D addresses cheating by personation using a communication device or computer resource, subject to the statutory elements.

5.3 Unauthorised access, malware and ransomware

Unauthorised access and damage to computer resources may attract provisions of the Information Technology Act, including Sections 43 and 66 depending on the conduct and required mental element. Malware can steal information, spy on users or disrupt systems. Ransomware encrypts or threatens to disclose data to pressure a victim into payment. Organisations should maintain offline or protected backups, apply security updates, restrict access and establish incident-response plans.

5.4 Cyberstalking, harassment and unlawful content

Digital platforms may be used for stalking, threats, harassment, doxxing, non-consensual sharing of intimate material and abuse targeting women or children. Depending on the facts, relevant provisions may be found in the Information Technology Act and general criminal law. A case must be assessed on its specific facts; not every offensive or disturbing online communication automatically constitutes a criminal offence.

5.5 Data theft, cyberattacks and attacks on critical systems

The theft of commercial or personal data can cause financial loss, expose confidential information and undermine trust. Attacks on essential services or protected systems can have

wider public consequences. Section 70B of the Information Technology Act establishes CERT-In's role as the national agency for responding to specified cybersecurity incidents; other provisions address protected systems and cyber terrorism where the statutory conditions are met.

6. LEGAL FRAMEWORK GOVERNING CYBERCRIME

6.1 Information Technology Act, 2000

The Information Technology Act, 2000 is India's central legislation dealing specifically with electronic records, electronic transactions and a range of computer-related offences. Important provisions include Sections 43 and 66 concerning specified unauthorised acts and computer-related offences; Sections 66C and 66D concerning identity theft and cheating by personation; Section 66E concerning violation of privacy; Section 66F concerning cyber terrorism; Sections 67, 67A and 67B concerning specified unlawful electronic content; Section 69A concerning blocking of public access to information under statutory conditions; and Section 70B concerning CERT-In. The precise section applied depends on the facts and legal elements.

Section 66A, which criminalised certain online messages, was struck down by the Supreme Court in *Shreya Singhal v. Union of India* (2015). It must not be treated as a valid offence. The judgment is a key reminder that cyber regulation must comply with constitutional protections.

6.2 Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 replaced the Indian Penal Code as the principal general criminal statute. Where cyber-enabled conduct also satisfies the elements of offences such as cheating, forgery, extortion, intimidation or stalking, the relevant provisions of the BNS may apply alongside the Information Technology Act, subject to rules against duplicative punishment and the facts of the case. Investigators should identify the specific offence and not assume that every online wrong is automatically a cyber offence under one particular statute.

6.3 Bharatiya Sakshya Adhiniyam, 2023 and electronic evidence

The Bharatiya Sakshya Adhiniyam, 2023 provides the current general framework for evidence, including electronic and digital records. Electronic evidence may include emails, chat logs, transaction records, server logs, CCTV files, device data and social-media content. Its admissibility and evidentiary weight depend on statutory requirements, authenticity, integrity and the circumstances in which it was obtained. Investigators should document

collection methods, preserve original data where possible, maintain chain of custody and use appropriate forensic procedures.

6.4 Digital personal data and intermediary rules

The Digital Personal Data Protection Act, 2023 is relevant to the processing of digital personal data, subject to its provisions, commencement and applicable rules. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended, set obligations for intermediaries within their scope. These instruments do not replace criminal investigation, but they may affect data security, grievance handling, content-related processes and the responsibilities of organisations.

7. CONSTITUTIONAL PROTECTION AND JUDICIAL PRINCIPLES

Article 14 of the Constitution protects equality before the law and equal protection of the laws. Article 19 protects specified freedoms, including speech and expression, subject to constitutionally permitted restrictions. Article 21 protects life and personal liberty and has been interpreted to include privacy. These guarantees are relevant to cybercrime investigation, surveillance, content restrictions and the handling of personal data.

In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court recognised privacy as a fundamental right. In Shreya Singhal v. Union of India (2015), the Court struck down Section 66A of the Information Technology Act and discussed the constitutional limits of restrictions on online speech. These decisions do not eliminate the State's ability to investigate crime; they require that state action have a lawful basis and respect constitutional safeguards.

8. REPORTING, INVESTIGATION AND ELECTRONIC EVIDENCE

Victims should preserve messages, URLs, screenshots, transaction IDs, bank statements, emails, phone numbers and other relevant records. In financial fraud, immediate contact with the bank and prompt reporting through helpline 1930 may improve the possibility of freezing or tracing funds, although recovery is not guaranteed. Complaints may also be submitted through the official National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>. Complaints are handled by the relevant law-enforcement authorities.

Investigators should promptly seek lawful preservation of relevant records, establish a timeline, trace transactions and devices, and document how evidence was collected. Digital evidence is fragile: files may be altered, logs may expire, and cloud data may be located abroad. Requests to service providers must follow applicable law and procedures.

International cooperation may be necessary where offenders, platforms or servers are outside India.

9. INSTITUTIONAL MECHANISMS

CERT-In is India's national agency for responding to specified cybersecurity incidents under Section 70B of the Information Technology Act. The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, supports coordination, training, analysis and cybercrime response. The National Cyber Crime Reporting Portal enables citizens to submit complaints online, including complaints involving financial fraud and crimes against women and children. Banks, payment providers, telecom operators and State police also play important roles in prevention and response.

10. MAJOR CHALLENGES

- Cross-border jurisdiction: offenders, infrastructure, victims and evidence may be located in different countries.
- Under-reporting and delayed reporting: victims may feel ashamed, fear exposure or not know where to complain.
- Technical capacity: police stations and courts may have unequal access to trained personnel, forensic tools and secure laboratories.
- Attribution difficulties: criminals use fake accounts, stolen identities, compromised devices and money-mule networks.
- Evidence integrity: electronic records can be deleted, modified or collected without adequate documentation.
- Rapid technological change: criminal methods evolve faster than training, public awareness and legal processes.
- Rights and proportionality: investigative powers must be exercised consistently with privacy, due process and freedom of expression.

11. RECOMMENDATIONS FOR REFORM

11.1 Strengthen cybercrime investigation

Provide continuing training in digital forensics, cryptocurrency tracing, cloud evidence and incident response, with adequate equipment and specialist units.

11.2 Improve victim support

Promote awareness of helpline 1930 and the official reporting portal, provide clear guidance on evidence preservation, and create accessible support for vulnerable victims.

11.3 Improve coordination

Develop timely protocols among police, banks, payment providers, telecom operators, CERT-In and relevant international authorities, subject to lawful safeguards.

11.4 Protect electronic evidence

Use standard procedures for collection, hashing, storage, access control and chain of custody, and ensure that forensic conclusions are transparent and reviewable.

11.5 Clarify legal duties

Periodically review cyber laws and subordinate rules to address new forms of fraud, AI-enabled impersonation and attacks on essential systems, while avoiding vague offences.

11.6 Safeguard civil liberties

Ensure surveillance, blocking and data-access measures have a clear legal basis, are necessary and proportionate, and provide appropriate oversight and remedies.

11.7 Improve public and business cybersecurity

Encourage multi-factor authentication, secure backups, timely software updates, staff training, incident plans and responsible disclosure of vulnerabilities.

12. CONCLUSION

Cybercrime is a serious challenge for a society that increasingly depends on digital services. India has an important legal foundation in the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and related data-protection and intermediary rules. Yet laws alone cannot ensure effective enforcement. Prevention requires digital literacy and secure systems; investigation requires technical expertise and reliable evidence; prosecution requires fair procedures; and victims need fast, accessible reporting and meaningful support.

A balanced approach should combine effective enforcement with constitutional rights, transparency and accountability. Better inter-agency coordination, stronger forensic capacity, prompt financial-fraud reporting, public awareness and periodic legal review can make India's cybercrime response more effective without weakening the rule of law.

13. BIBLIOGRAPHY

1. The Information Technology Act, 2000, India Code, Government of India:
<https://www.indiacode.nic.in/indiacode/handle/123456789/1999>
2. The Bharatiya Nyaya Sanhita, 2023, India Code, Government of India.
3. The Bharatiya Sakshya Adhinyam, 2023, India Code, Government of India.
4. The Digital Personal Data Protection Act, 2023, India Code, Government of India.
5. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
6. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
7. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
8. Indian Computer Emergency Response Team (CERT-In), official website and directions:
<https://www.cert-in.org.in/>
9. National Cyber Crime Reporting Portal, Government of India: <https://cybercrime.gov.in/>
10. Press Information Bureau, Government of India, “Additional National Measures for Data Security” (official press note):
<https://www.pib.gov.in/PressNoteDetails.aspx?ModuleId=3&NoteId=157093>