

International Journal Research Publication Analysis

Page: 01-02

CYBER CRIME IN INDIA: LEGAL FRAMEWORK, CHALLENGES AND REFORMS

***Poonam Prajapati**

B Wing 206, Madhav residency 2, dandiwad faliya balitha vapi

Article Received: 16 September 2026

*Corresponding Author: Poonam Prajapati

Article Revised: 06 October 2026

B Wing 206, Madhav Residency 2, Dandiwad Faliya Balitha Vapi.

Published on: 26 October 2026

DOI: <https://doi-doi.org/101555/ijrpa.5321>

ABSTRACT

The rapid expansion of the internet, smartphones, digital payments, social media and online services has transformed modern society. India has experienced particularly rapid digitalisation, with citizens increasingly using digital platforms for banking, education, communication, commerce and government services. However, the growth of the digital environment has also created opportunities for criminal activity. Cyber crimes such as identity theft, online financial fraud, hacking, phishing, cyber stalking, ransomware, data theft, online sexual exploitation and cyber terrorism have emerged as serious legal and social challenges.

1. INTRODUCTION

Unlike conventional crimes, cyber crimes can be committed anonymously, across geographical boundaries and with considerable speed. Evidence may be stored on servers located in different countries, while perpetrators may use sophisticated technologies to conceal their identities. These characteristics create significant difficulties for investigation, prosecution and enforcement.

India's principal legislation dealing specifically with cyber offences is the Information Technology Act, 2000. Its provisions cover computer-related offences, identity theft, cheating by personation, privacy violations, cyber terrorism and certain forms of unlawful electronic content.

The Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, also operates alongside the Information Technology Act where conduct constitutes a general criminal offence. The Digital Personal Data Protection Act, 2023 and the Digital Personal Data

Protection Rules, 2025 further strengthen the regulatory framework relating to personal data and digital privacy.

2. SCOPE AND OBJECTIVES OF THE ARTICLE

This article examines the meaning and major forms of cyber crime in India, the existing legal framework, constitutional protections, important judicial decisions, problems relating to electronic evidence and investigation, institutional mechanisms such as CERT-In and the National Cyber Crime Reporting Portal, and the reforms required to make India's cyber-law framework more effective.

3. KEYWORDS: Cyber Crime; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Digital Personal Data Protection Act, 2023; Cyber Security; Privacy; Electronic Evidence; Cyber Law; India.

4. STRUCTURE OF THE STUDY

1. Meaning and Nature of Cyber Crime
2. Major Forms of Cyber Crime in India
3. Legal Framework Governing Cyber Crime
4. Constitutional Protection of Privacy and Digital Rights
5. Important Judicial Decisions
6. Electronic Evidence and Investigation
7. Institutional Mechanisms for Cyber Crime Prevention
8. Major Challenges in Enforcement
9. Need for Legal and Institutional Reforms
10. Conclusion
11. Bibliography