The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

CYBER CRIMES AND LEGAL REMEDIES IN INDIA

Subhasri Roy

Introduction

The rapid growth of digital technology and internet connectivity has transformed modern society. Online banking, digital payments, social media platforms, e-commerce websites, and cloud-based communication systems have made life more convenient and connected. However, along with technological advancement, cyber crimes have also increased significantly. Cyber crimes refer to unlawful acts committed through computers, digital devices, or internet networks. These offences may target individuals, businesses, financial institutions, or even government systems.

India has become one of the fastest-growing digital economies in the world. With the expansion of digital platforms and smartphone usage, cyber offences such as hacking, phishing, identity theft, online fraud, cyberbullying, data breaches, and online harassment have become common. These crimes not only cause financial loss but also affect privacy, mental health, and public security. Therefore, effective legal remedies and strong cyber laws are necessary to protect individuals and maintain cyber security.

Meaning and Nature of Cyber Crime

Cyber crime refers to any illegal activity involving computers, digital devices, or communication networks. In cyber crimes, technology may either be the target of the offence or the tool used to commit the offence. Unlike traditional crimes, cyber crimes can be committed from any location and often involve anonymous offenders, making investigation difficult.

Cyber crimes may be committed against individuals, organisations, or government institutions. Due to the global nature of the internet, cyber criminals may operate across national

boundaries, which further complicates legal enforcement and investigation.

Types of Cyber Crimes

One of the most common cyber crimes in India is online financial fraud. Fraudsters often deceive people through fake messages, fraudulent websites, and phishing emails in order to steal banking information, passwords, or OTP details. Many people lose money through fake investment schemes, digital payment frauds, and online shopping scams.

Identity theft is another serious cyber offence. Criminals misuse personal information such as Aadhaar details, debit card numbers, or social media accounts to commit fraud or impersonation. Such offences violate the privacy and security of individuals.

Cyberbullying and online harassment have also increased rapidly, especially on social media platforms. Individuals may face abusive messages, threats, character assassination, or circulation of morphed images online. Women and children are particularly vulnerable to such crimes.

Hacking refers to unauthorized access to computer systems or networks. Hackers may steal confidential information, alter data, or disrupt digital services. Government databases, banking systems, and corporate servers are frequent targets of cyber attacks.

Another growing concern is the circulation of fake news and deepfake content. Manipulated videos and false online information may create panic, damage reputations, and disturb public order. Such misuse of technology creates serious legal and ethical concerns.

Legal Framework Governing Cyber Crimes in India

The primary legislation dealing with cyber crimes in India is the Information Technology Act, 2000. The Act was enacted to provide legal recognition to electronic transactions and regulate cyber offences. Several amendments have strengthened the law over time.

Section 43 of the Information Technology Act imposes liability for unauthorized access, downloading of data, introduction of viruses, and damage to computer systems. Section 66 provides punishment for computer-related offences committed dishonestly or fraudulently.

Identity theft is punishable under Section 66C, while cheating by personation through electronic means is punishable under Section 66D. Section 67 deals with the publication or transmission of obscene material in electronic form. These provisions are important in addressing online abuse and illegal digital content.

The Bharatiya Nyaya Sanhita, 2023 also becomes relevant in cases involving online cheating, criminal intimidation, defamation, forgery, and publication of false information. Traditional

criminal law principles continue to apply even when offences are committed through digital means.

The Digital Personal Data Protection Act, 2023 further strengthens privacy protection by regulating the collection and processing of personal digital data. Companies handling user data are expected to maintain security safeguards and protect personal information from misuse.

Role of Law Enforcement Agencies

Cyber crime investigation requires technical expertise and specialised infrastructure. In India, cyber crime cells have been established in several states to investigate digital offences. The Indian Cyber Crime Coordination Centre (I4C) was also established by the Ministry of Home Affairs to improve coordination and strengthen cyber crime prevention.

Citizens may report cyber financial frauds and online offences through the National Cyber Crime Reporting Portal. This platform helps victims file complaints relating to cyberbullying, hacking, online fraud, and digital harassment.

Despite these developments, cyber crime investigation still faces challenges due to lack of technical awareness, shortage of trained personnel, and jurisdictional difficulties. Since cyber offences often involve international networks, effective cooperation between countries becomes necessary.

Challenges in Combating Cyber Crimes

One of the biggest challenges in cyber law enforcement is the anonymous nature of the internet. Criminals may hide their identities using fake accounts, VPN services, or encrypted communication systems. This makes identification and prosecution difficult.

Another challenge is the lack of awareness among internet users. Many people unknowingly share confidential information or fall victim to fraudulent schemes due to limited cyber security knowledge.

Rapid technological advancement also creates legal difficulties because laws often fail to keep pace with emerging cyber threats. New forms of cyber offences such as ransomware attacks, cryptocurrency fraud, and AI-generated scams are increasing rapidly.

Digital evidence management is another complex issue. Preservation, collection, and authentication of electronic evidence require technical expertise and proper legal procedures. Courts must also adapt to evolving technological realities while ensuring fair trial standards.

India also faces challenges relating to digital evidence and delayed investigation procedures. Electronic evidence can easily be altered, deleted, or transferred across different servers within

seconds. Therefore, proper preservation and authentication of digital evidence become extremely important during cyber crime investigations. Courts also require technical experts to understand complex digital systems and cyber forensic reports. In many cases, victims hesitate to report cyber offences due to fear, embarrassment, or lack of awareness regarding legal remedies. This creates underreporting of cyber crimes and weakens enforcement efforts. Furthermore, small businesses and local institutions often lack sufficient cyber security infrastructure, making them easy targets for online attacks and financial frauds.

Preventive Measures and Cyber Awareness

Preventing cyber crime requires both legal regulation and public awareness. Individuals should use strong passwords, avoid suspicious links, verify online transactions, and regularly update security software. Social media users must be cautious while sharing personal information online.

Educational institutions and organisations should conduct cyber awareness programmes to promote responsible internet usage. Businesses must implement proper cyber security measures and data protection systems to prevent breaches and financial loss.

Social media companies and digital platforms also have an important responsibility in preventing cyber crimes. These companies should establish stronger content monitoring systems, quick grievance redressal mechanisms, and better privacy safeguards for users. Artificial intelligence and cyber forensic tools may also be used by law enforcement agencies to identify suspicious online activities and prevent digital frauds at an early stage. Regular awareness campaigns through schools, colleges, and media platforms can help citizens understand safe online practices and reduce the risk of cyber victimisation.

The government should continue strengthening cyber infrastructure, digital literacy, and legal enforcement mechanisms. International cooperation is also necessary because many cyber crimes operate beyond territorial boundaries.

Conclusion

Cyber crimes have become one of the most significant challenges in the digital age. While technology has improved communication, business, and governance, it has also created opportunities for criminal misuse. Online fraud, hacking, cyberbullying, identity theft, and digital harassment continue to affect individuals and institutions across India.

India has established an important legal framework through the Information Technology Act, criminal laws, and data protection legislation. However, the constantly evolving nature of cyber

threats requires continuous legal reforms, stronger enforcement, and increased public awareness.

An effective balance between technological growth and cyber security is necessary for a safe digital society. Legal remedies alone are not sufficient unless citizens, institutions, and governments work together to promote cyber awareness, digital responsibility, and ethical use of technology.

Footnotes

2 Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

3 Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

4 The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

5 Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C), Government of India.

6 National Cyber Crime Reporting Portal, Government of India, https://cybercrime.gov.in (last visited May 16, 2026).

7 Shreya Singhal v. Union of India, (2015) 5 SCC 1.

8 Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.